IDEAS | PEOPLE | TRUST

BDO Financial Services Quarterly Update

Q2 2025

Welcome to your Quarterly Financial Services Sector Update

BDO's Quarterly Financial Services Sector Update summarises the key regulatory developments and emerging business risks relevant for all financial services firms, including banks, building societies, investment and wealth managers, payments and insurance providers.

Our FS Advisory Services team works with a broad range of financial services firms as advisors, giving us an extensive 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 help inform your oversight and assurance activities over the firm's priority risks.

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.

Editorial team

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

Sam Ewen
Manager, FS Advisory

sam.ewen@bdo.co.uk

Adam Watson
Associate Business Development Manager

+44 (0)7443 373 993
adam.watson@bdo.co.uk

Your BDO Financial Services Advisory Team

Our Financial Services Advisory team provides consultative problem solving together with core regulatory, governance, internal audit, risk management and resourcing services to meet the needs of your business. Our team combines skills and experience from industry and regulatory backgrounds, enabling us to provide robust and proportionate advice to our clients. We strive to be a trusted adviser who can be relied upon to add value, provide ideas and to challenge and deliver a service which will contribute to your business' success.

Regulatory & Governance

Leigh Treacy
Partner, Head of FS Advisory

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

Richard Barnwell
Partner

+44 (0)7717 214 818
richard.barnwell@bdo.co.uk

Fiona Raistrick
Partner

+44 (0)7929 057 616
fiona.j.raistrick@bdo.co.uk

Mads Hannibal
Partner

+44 (0)7810 836 222
mads.hannibal@bdo.co.uk

Internal Audit & Assurance

Chris Bellairs
Partner

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

Luke Patterson
Partner

+44 (0)7929 058 083
luke.patterson@bdo.co.uk

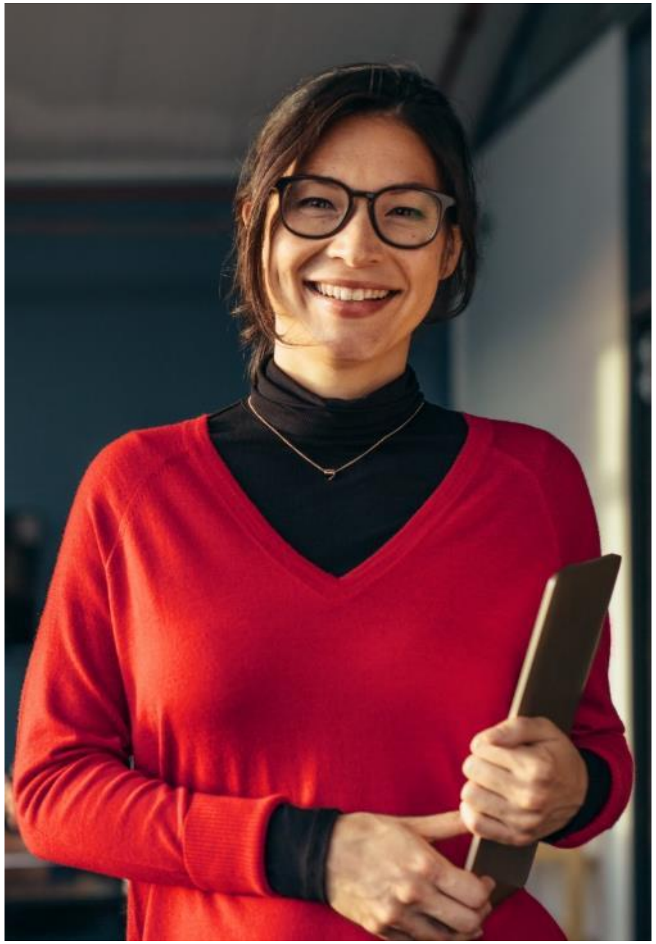
Sam Patel
Partner

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

Sam Cornish
Partner

+44 (0)7502 276 555
sam.cornish@bdo.co.uk

Your BDO Financial Services Advisory Team



North of England

Paul Gilbert
Partner

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

Scotland

Mick Campbell
Partner

+44 (0)7500 025 243
mick.campbell@bdo.co.uk

ESG & Accounting Advisory

Sasha Molodtsov
Partner

+44 (0)7581 478 087
sasha.Molodtsov@bdo.co.uk

Mark Spencer
Partner

+44 (0)7718 864 980
mark.spencer@bdo.co.uk

Contents

01

All Financial Services

Back to contents

Regulatory grid - What is on the regulatory change horizon

On 14 April, the Bank of England, FCA, PRA and other regulators published the latest Regulatory Initiatives Grid which provides the regulatory pipeline for the next 24 months allowing stakeholders to see what is in development. This is the first grid published since 2023 making it the first since the new Government was elected in July 2024 and it reflects the Government's growth agenda. In addition, the FCA published its next five-year strategy on 25 March 2025 highlighting four themes focused on internal efficiencies, supporting sustainable growth, supporting consumers navigate their financial lives, and fighting financial crime. In this article we look at some of the new, more significant initiatives for the financial sector.

Regulatory Initiatives Grid - April 2025

Richard Barnwell
Partner

richard.barnwell@bdo.co.uk

The initiatives grid is a substantial document of some 80 pages, and the aim of this article is to assist firms in digesting this information to focus on the key regulatory changes on the horizon. Firms will be reassured that many of the initiatives relate to known topics which have been carried forward from the previous grid. About 15% of the content relates to initiatives completed or discontinued, the most notable being the FSCS compensation framework review which has been deprioritised.

The grid does not include supervisory, or enforcement matters and is instead focused on policy-related initiatives. Of the 144 initiatives, 69% are low impact, 17% are high impact and 20% are unknown impact (these include market studies which have not yet concluded). The FCA and PRA have the highest volume of high impact initiatives and the most initiatives overall. A key feature of the grid published in April is that it now has a useful dashboard function which enables firms to easily search through the data. Regulatory Initiatives Grid dashboard - April 2025 | FCA.

There are only a small number of significant new initiatives that were not on the previous grid, and we summarise these initiatives below.

Consumer Duty

The FCA has long signalled it would consider how to rationalise its Handbook of rules and guidance in light of the Consumer Duty, but if the market is looking for a radical slim down of the Handbook this announcement may be more of a cause for disappointment than celebration.

Rather, it reads as a cautious but none the less helpful set of initiatives, and the Feedback Statement is a compendium of initiatives. It consolidates what is already underway as well as producing some additional areas for review. There is an expedited consultation process to get these changes adopted quickly areas for action and further plans for revie. FS25/2: Immediate wing FCA requirements following introduction of the Consumer Duty. These changes should be genuinely helpful in giving clarity to firms and limiting some of the more challenging parts of the consumer duty, such as responsibilities across a supply chain. Other changes are welcome housekeeping.

Stress testing

For banks and major insurers, significant stress testing exercises will be conducted in 2025 which form the basis for testing the resilience of the UK financial system.

Banks: A bank capital stress test will be run in 2025 by the Bank of England in which the largest and most systemic UK banks will participate. This exercise will test the risks related to the financial cycle and will inform the setting of capital buffers for the banking system and for individual banks, the capital stress exercises will look at resilience.

continued >

Back to contents

Regulatory grid - What is on the regulatory change horizon

Major life insurers:
The objectives for the 2025 stress test are:

1. Assess sector and individual firm resilience to severe but plausible events.

2. Strengthen market understanding and discipline through individual firm publication.

3. Improve insight into risk management vulnerabilities.

Results will be provided individually to firms and published on an aggregate basis.

Insurers liquidity reporting

The PRA is improving its regulation and supervision of insurers' liquidity risks. Its current initiative is developing proposals to introduce new reporting requirements on the insurance firms with the largest exposures to liquidity risk. This will enable it to more effectively supervise insurers' liquidity risk by providing timely, consistent and accurate information. Final implementation from year end 2025.

PEPS

As firms will be aware, the FCA has a statutory obligation (FSMA s78) to review firms' adherence to the FCA politically exposed person (PEP) Guidance (FG 17/6) and report by end June 2024.

Regulation of Crypto assets

The FCA will lead on the creation of a new regime for crypto assets. Following Treasury legislation being laid, new RAO Activities will come into the FCA's remit, alongside an Admissions and Disclosure and Market Abuse regimes. The FCA's Cryptoasset Roadmap sets out the planned FCA publications for the rules and requirements to implement this new regime. There are significant number of initiatives related to the regulation of crypto assets that will come under the FCA's scope, including at least one discussion paper and four consultation papers planned for this year.

Smart Data - Open banking

The FCA and Treasury will publish a roadmap for the roll out of Open Finance, and they expect the regulatory foundations for the first scheme to be in place by the end of 2027.

Introduction of T+1 standard settlement cycle for securities Trades

The Accelerated Settlement Technical Group published its final report early in February 2025. The Government published its response later that month, announcing it will legislate for T+1 to be mandatory from 11 October 2027. A joint press statement from the Government, the FCA and the Bank was also published confirming cross-authority support for the move to T+1. Firms should now begin preparations for 11 October 2027 to be the first day of trading under a T+1 standard.

Repeal and replace of the requirements on central counterparties as set out in Titles III, IV and V of the European Market Infrastructure Regulation (EMIR)

The Bank intends to publish consultations on its new rules alongside a Treasury statutory instrument setting out the relevant repeal and restatement of assimilated law, in Q2/Q3 and Q4 2025. Relevant Treasury legislation and Bank rules will then be taken forward in 2026.

There are several significant initiatives still underway, including addressing the Advice Gap, regulating BNPL, and establishing a new safeguarding regime for payments and e-money institutions. Efforts are also ongoing for ESG ratings regulation and sustainable disclosures.

While the grid might not bring many new, significant initiatives, it's crucial for firms to pause and reflect on these regulatory changes. How do they affect your operations? Where can you find opportunities for improvement? How can these changes help you align your strategies with new standards to enhance compliance and resilience? Considering these questions today will help you navigate the regulatory landscape and position your firm to succeed.

If you require support or would like to discuss with any of these topics, please contact:

richard.barnwell@bdo.co.uk

National Crime Agency releases its 2025 National Strategic Assessment of Serious and Organised Crime

The National Crime Agency ("NCA") released its latest National Strategic Assessment ("NSA") of Serious and Organised Crime ("SOC") in March 2025. The NSA 2025 provides a comprehensive analysis of the evolving threats posed by serious and organised crime in the UK, serving as a crucial resource for law enforcement agencies, policymakers, and private sector stakeholders.

Vladimir Ivanov
Associate Director, FS Advisory

vladimir.ivanov@bdo.co.uk

In March 2025, the NCA released its NSA of Serious and Organised Crime 2025. The NSA 2025 outlines the current landscape of criminal activities and informs strategic responses to mitigate these threats. They key areas of concern for financial services firms are as follows:

Overall Threat Landscape
While the overall SOC threat to the UK increased in 2024, the rate of increase has slowed compared to previous years

- This growth in serious and organised crime is principally being driven by online connectivity and the growth of technology
- Online connectivity underpins a wide variety of offending including child sexual abuse, cybercrime, and fraud, and enables almost all serious and organised criminality in some form
- Developments in technology and artificial intelligence are likely to be increasing the speed and volume of offending, as well as the level of harm caused to victims.

Fraud

- Fraud continues to be the most prevalent crime against individuals in England and Wales, accounting for an estimated 41% of all crimes as per the Crime Survey for the year ending September 2024
- Only an estimated 14% of frauds against individuals are reported to Action Fraud or the police
- Investment fraud and romance fraud reports continue to be at the high levels seen during the pandemic, with courier fraud and payment diversion fraud still below pre-pandemic levels, although victim harm from both remains high
- Many frauds impacting UK victims have an overseas element
- It is estimated that 67% of fraud reported in the UK is cyber-enabled, with authorised push payment frauds continuing to be driven by the abuse of online platforms. The cyber-enabled nature of many frauds and the methods used to launder the criminal proceeds often involve multiple jurisdictions
- Phishing attacks remain prevalent, using tools with ever more sophisticated technical features to bypass security measures and counter the increased public awareness and understanding of fraud risk

continued >

National Crime Agency releases its 2025 National Strategic Assessment of Serious and Organised Crime

- Criminals continue to search for innovative ways to reduce the effectiveness of countermeasures, including fraudulent schemes designed to add stolen card details to digital wallets on criminally controlled mobile phones through intercepting one-time passcodes, either via social engineering or malware
- Criminals continue to adopt generative artificial intelligence to enhance the sophistication of fraud attacks against individuals and businesses, although they are currently used to enhance existing threats rather than create entirely new ones. The use of deepfake videos and voice cloning has been used to enable CEO frauds against large businesses.

Illicit Finance

- It is thought that over £12 billion of criminal cash is generated each year in the UK and it is a realistic possibility that over £100 billion is being laundered through and within the UK or UK-registered corporate structures each year.
- UK corporate structures continue to enable money laundering due to vulnerabilities in their creation and oversight. While it is too early to see impact from the phasing in of new powers for Companies House under the Economic Crime and Corporate Transparency Act 2024, it is hoped that the introduction of measures such as identity verification for company Directors, Persons with Significant Control, and Authorised Corporate Service Providers will displace some criminals from using UK corporate structures.
- Organised Criminal Groups and money launderers are aware that washing large amounts of funds through the financial system will trigger concerns with financial institutions, and criminals have therefore become adept at transferring funds in other ways. The most significant method for doing this remains Trade-Based Money Laundering (“TBML”). The NCA estimates that it is likely that over £10 billion a year is moved through TBML schemes impacting on the UK.
- Accounts at UK banks and non-bank payment service providers continue to be exploited by money laundering networks, including for ‘money mule’ activity.
- Money laundering through the capital markets, such as buying and selling of financial instruments continues to offer a route for criminals to move and disguise the audit trail of money through the use of complex financial transactions.
- The scale of activity by the Russian-speaking money laundering networks is highly likely greater than previously reported. They provide cash to cryptocurrency conversions in the UK and overseas; launder funds for transnational organised crime groups; enable Russian elites and entities to evade UK financial sanctions; and have funded Russian espionage operations.

What does this mean for firms

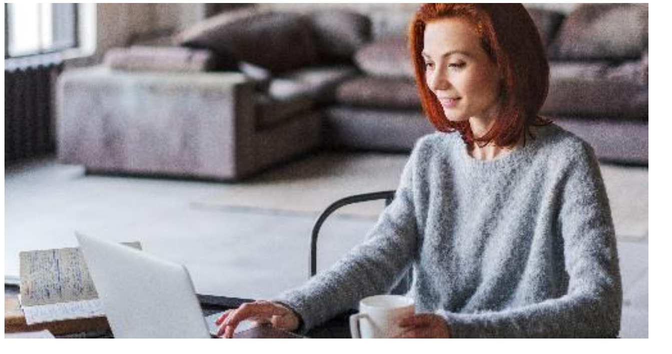
The NSA 2025 underscores the dynamic and multifaceted nature of serious and organised crime threats facing the UK. It emphasises the necessity for adaptive, collaborative, and intelligence-led responses to effectively mitigate these evolving challenges.

The NSA 2025 has significant implications for financial services firms, providing actionable insights to shape risk management, compliance, and financial crime strategies.

Including:

- Financial services remain key conduits and battlegrounds in the fight against serious and organised crime. Firms must continue to enhance AML, CTF, and sanctions compliance frameworks to address emerging threats identified by the NSA, including trade-based money laundering and crypto-enabled laundering

continued >

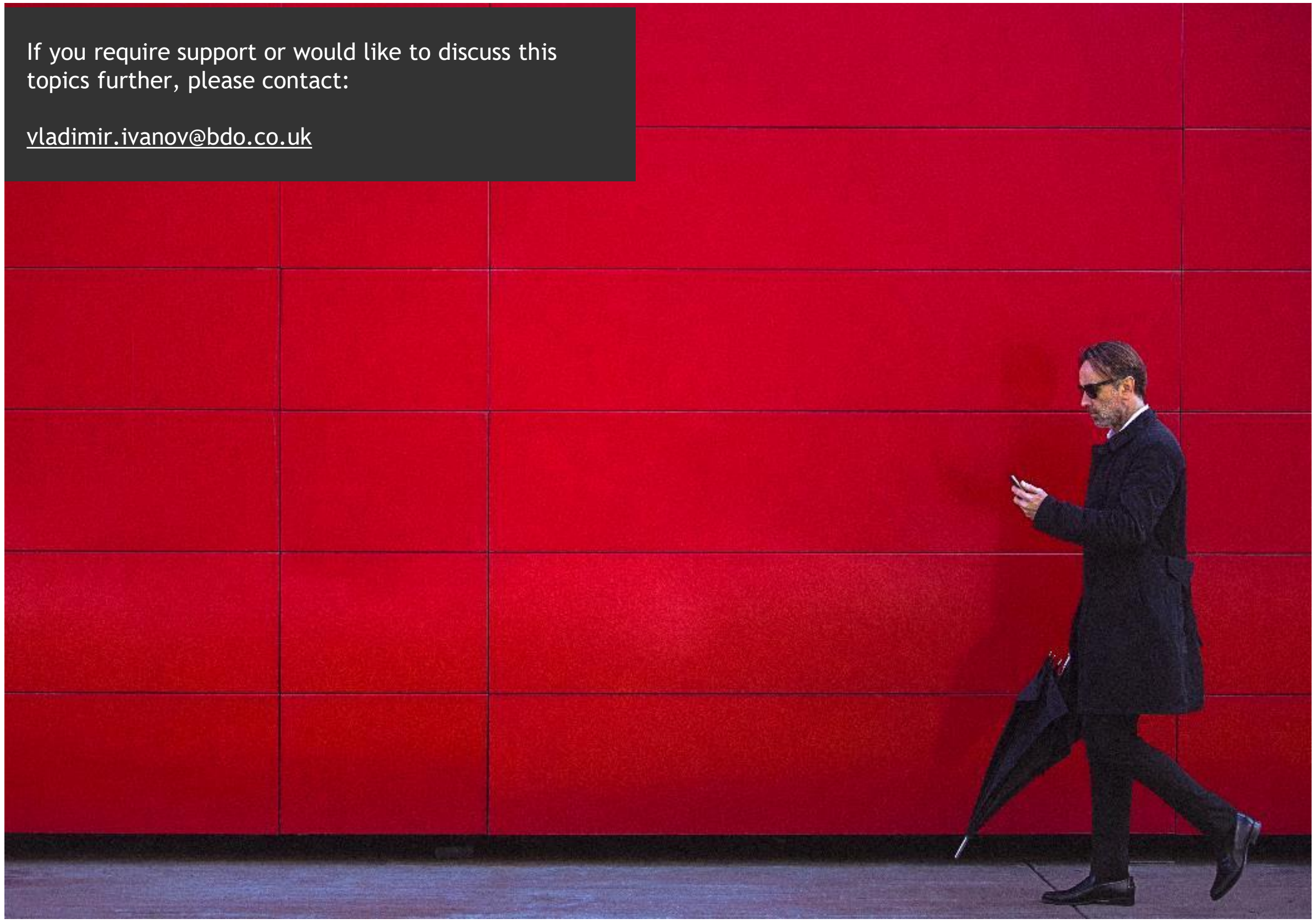


National Crime Agency releases its 2025 National Strategic Assessment of Serious and Organised Crime

- Fraud continues to be an escalating threat. Given the perfect storm of heightened regulatory pressures and the diabolical increase of fraud, firms must ensure they have robust Fraud Risk Management frameworks which can not only stand up to regulatory scrutiny, but can also protect firms and their customers from illicit actors
- Firms should use the NSA as part of their strategic risk forecasting. The NSA isn't just a retrospective—it's a forward-looking tool. Therefore, firms should:
  - use it to inform their Business-Wide Risk Assessments ("BWRAs")
  - (where possible) map NSA-identified threats to control testing, customer segmentation, and audit priorities.

If you require support or would like to discuss this topics further, please contact:

vladimir.ivanov@bdo.co.uk



R&D tax relief - consultation on advanced clearances

As part of the Spring Statement on 26 March 2025, the Government launched a consultation to explore the potential for "widening the use of advance clearances in the R&D tax reliefs". The key themes of the consultation are whether such a system can effectively reduce error and fraud in R&D tax reliefs while also providing R&D claimants with greater certainty around their return on R&D investment, and an improved customer experience in terms of HMRC's approach to their claims.

Carrie Rutland
Head of FS R&D

carrie.rutland@bdo.co.uk

Romane Reeves
Associate Tax Director

romane.reeves@bdo.co.uk

Why a new advance assurance system is needed

The R&D tax relief regimes have an existing advance assurance scheme. However, this has proved ineffective, and the uptake has consequently been very low. Only 80 applications were received in 2023/24, and it seems clear that the balance of time and effort required by the business versus the level of certainty obtained is not attractive. In addition, the current scheme is only available to SMEs (businesses with turnover below £2 million and fewer than 50 employees).

New clearance options

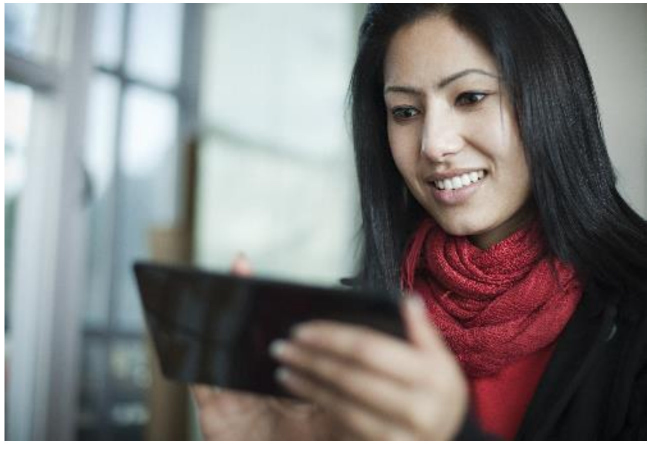
The consultation aims to explore the benefits and drawbacks of both voluntary and mandatory assurances. Voluntary assurances may be most appealing to companies seeking certainty around the technical basis for their claims, whilst mandatory assurances could be more targeted in reducing fraud and error.

In addition, the Government is also considering three stages at which advance assurance could be provided, as follows:

- Pre-activity: early discussions between companies and HMRC to identify and address uncertainties before R&D activities commence
- Pre-claim: assurance sought closer to the time of claim submission when R&D activities are underway, allowing for more detailed scrutiny of the work being undertaken
- Pre-payment: companies could request checks before payment of credits to ensure that claims are compliant and reduce the risk of having to repay funds later.

On the face of it, pre-activity clearances might be most beneficial for businesses in the payments and e-money sector as they would enable R&D investment decisions to be made with more certainty. However, with all projects, there is always the possibility that 'unforeseen R&D' may arise. Therefore, even an advance clearance after a claim has been made but before payment, may be beneficial: e.g. giving the business the certainty of knowing that HMRC will not open an enquiry into the claim and seek to claw back R&D tax credits.

continued >



R&D tax relief - consultation on advanced clearances

Who will be eligible?

The Government acknowledges that a full advanced assurance for all claimant companies is not feasible due to limited resources and expertise within HMRC. Therefore, it is likely that eligibility for advanced clearance will be limited to certain types of business. For example, one option is to focus clearances on growing and high-potential companies or companies working in key sectors identified in the Government's Industrial Strategy. The government has identified both financial services, and digital and technologies as a 'growth driving sectors' so firms operating within all sub-sectors of the financial services sector would be eligible for a new voluntary advance assurance system if voluntary assurances are targeted that way.

However, small business in the sector may also find themselves subject to new mandatory assurances. These would be targeted at business groups with high non-compliance rates and HMRC's research identifies small businesses as most likely to make errors in R&D claims.

Benefits for the FS sector

R&D activities and associated claims for tax relief are key to maintain competitiveness and meet evolving customer needs. An effective advance assurance system could provide increased certainty and allow businesses to plan their R&D activities and manage the associated cashflows more effectively, so would be particularly helpful for those businesses with significant tech investment.

The Government also view the assurance process as being a way to simplify the R&D claims procedure, which could be particularly beneficial in such a fast-paced and evolving sector.

Issues and timescale

The consultation acknowledges that it will not have the resources to create an all-encompassing R&D clearances system, and it is the lack of resources and expertise within HMRC that is the main concern over how effective the new advanced assurance system may be.

We believe it will be difficult for HMRC to design a system which will add value to all claimants and potential claimants within the sector. However, a phased approach to mandatory assurance on a focused, sector and topic basis may add some value. For example, advanced assurance may be helpful to confirm the impact of legislative changes introduced in the 'Merged R&D regime', effective for accounting periods commencing on or after 1 April 2024. The most relevant areas of uncertainty for businesses are:

- Which company can claim for qualifying R&D activity in scenarios where R&D is 'contracted out' between two parties
- Whether any of the exemptions to claim for 'Qualifying overseas activity' will apply. One of HMRC's examples of such activity is US based activity due to access regulations within the US banking sector.

Unlike the advance tax certainty consultation also published with the Spring Statement which focuses on 'Major projects', the R&D consultation sets no specific timeline for implementing a new system. Until one does materialise, it remains vital that businesses carrying out R&D take expert advice on the eligibility of their project for R&D relief and in compiling claims.

What this means for firms

The new advance assurance system for R&D tax relief could offer firms greater certainty in planning and managing their R&D activities, which is crucial for maintaining competitiveness and meeting evolving customer needs. Until these changes are implemented, firms should continue to seek expert advice on R&D relief eligibility and claims to ensure they maximise their opportunities.

BDO will be submitting a detailed response to the consultation which runs until 26 May 2025 and we encourage firms to respond as well by submitting this form.

If you require support or would like to discuss this topics further, please contact:

carrie.rutland@bdo.co.uk or romane.reeves@bdo.co.uk

Back to contents

Introduction to the IIA's Cybersecurity Topical Requirement

The new Cybersecurity Topical Requirement is mandatory when auditing relevant risks and must be used in conjunction with the Standards. Effective from 5 February 2026, it sets baseline expectations for governance, risk management, and control processes. Internal auditors are required to document the applicability of each requirement and justify any exclusions. Accompanied by a User Guide detailing practical applications and test procedures, this requirement aligns with established frameworks such as NIST and COBIT, supporting a consistent, industry-aligned approach to evaluating cybersecurity across organisations.

Steve Dellow
Director, BDO Digital

steve.dellow@bdo.co.uk

Overview of Topical Requirements

The International Professional Practices Framework ("IPPF") consists of the Global Internal Audit Standards ("Standards"), Topical Requirements, and Global Guidance. Because the Standards serve as the authoritative reference for required practices, Topical Requirements, used alongside the Standards, are deemed mandatory. Topical Requirements outline clear expectations for internal auditors by specifying a minimum baseline for the audit of particular risk topics. Adhering to these requirements is compulsory for assurance engagements and is recommended for advisory work.

A Topical Requirement applies in any of the following circumstances:

- The topic features as part of an engagement in the internal audit plan
- The topic arises during the execution of an engagement
- The topic becomes the subject of an engagement request not included in the original internal audit plan.

Overview of the Cybersecurity Topical Requirement

The Cybersecurity Topical Requirement offers a consistent and thorough method for evaluating the design and implementation of cybersecurity processes and controls and defines a minimum baseline for assessing cybersecurity within an organisation. The provision does not mandate internal audit functions to undertake specific cybersecurity audits, however, when cybersecurity reviews are performed, compliance with the requirement becomes mandatory. Internal audit functions have a one-year period to align with the requirements, which come into force on 5 February 2026.

The guidance is presented as two companion documents: the Topical Requirement and the corresponding Topical Requirement User Guide. The Topical Requirement outlines domain areas as an essential baseline for evaluating cybersecurity within an organisation. Under each domain, the document specifies a set of requirements that internal auditors are obliged to review. This element of the guidance is mandatory.

Building on that foundation, the User Guide offers further insights into how these requirements may be applied within each domain. In particular, it provides a step-by-step outline for undertaking a cybersecurity audit. Additionally, it maps the requirements to the NIST Cybersecurity Framework 2.0, COBIT 2019, and NIST 800-53, ensuring alignment with established industry standards.

continued >

Introduction to the IIA's Cybersecurity Topical Requirement

Finally, it includes a sample audit programme that can be used to support the development of specific audit test procedures. While this guidance is recommended for best practice, it is not compulsory.

The three key domains within the Topical Requirement are:

- **Governance**: Evaluating and Assessing Cybersecurity Governance
- **Risk management**: Evaluating and Assessing Cybersecurity Risk Management
- **Controls**: Evaluating and Assessing Cybersecurity Control Processes.

The key requirements under each domain are as follows:

Governance

- A formal cybersecurity strategy and objectives should be established, communicated and periodically updated
- Policies and procedures related to cybersecurity should be established and periodically updated
- Cybersecurity roles and responsibilities should be established and periodically reviewed to assess individuals' skills and capabilities
- Relevant stakeholders should regularly collaborate to address existing vulnerabilities and emerging cybersecurity threats.

Risk Management

- The organisation's risk assessment and risk management processes should include identifying, analysing, mitigating, and monitoring cybersecurity threats and their impact on achieving strategic objectives
- Cybersecurity risk management is conducted across the entire organisation and encompasses a range of areas
- Accountability and responsibility for cybersecurity risk management are established and effectiveness is monitored
- A prompt escalation process is in place for cybersecurity risks exceeding acceptable thresholds, taking into account both financial and nonfinancial impacts
- Cybersecurity risk awareness is conveyed throughout the organisation, with management undertaking periodic reviews of deficiencies and ensuring prompt remediation
- A robust cybersecurity incident response and recovery process is implemented, covering detection, containment, recovery, and post-incident analysis, and it is periodically tested to ensure effectiveness.

Controls

- Internal and vendor-based controls are implemented to safeguard confidentiality, integrity, and availability, with periodic evaluations ensuring alignment with cybersecurity objectives and prompt issue resolution
- A talent management process is in place to develop and maintain cybersecurity competencies through training, with periodic reviews ensuring its effectiveness
- A structured process is established to continuously monitor and report emerging threats and vulnerabilities, ensuring timely prioritisation and implementation of improvements in cybersecurity operations
- Cybersecurity considerations are integrated throughout the lifecycle of all IT assets, including hardware, software, and vendor services
- Processes are established to strengthen cybersecurity covering configuration, device administration, encryption, patching, user-access management and software development
- Comprehensive network-related controls are established, encompassing segmentation, firewalls, limited external connections, VPN/zero trust measures, IoT safeguards, and intrusion detection/prevention systems

continued >

Back to contents

Introduction to the IIA’s Cybersecurity Topical Requirement

- Endpoint-communication security controls are implemented for critical services such as email, browsers, videoconferencing, messaging, social media, and file sharing.

For internal auditors, this requirement constitutes a notable broadening of their remit. They are now expected to acquire deeper insight into cybersecurity, spanning technical considerations and risk management frameworks. This evolution necessitates continuous professional development through increased cyber security knowledge, and closer engagement with information security colleagues. In so doing, auditors will be better placed to assess cybersecurity risks and deliver tangible recommendations that support organisational objectives.

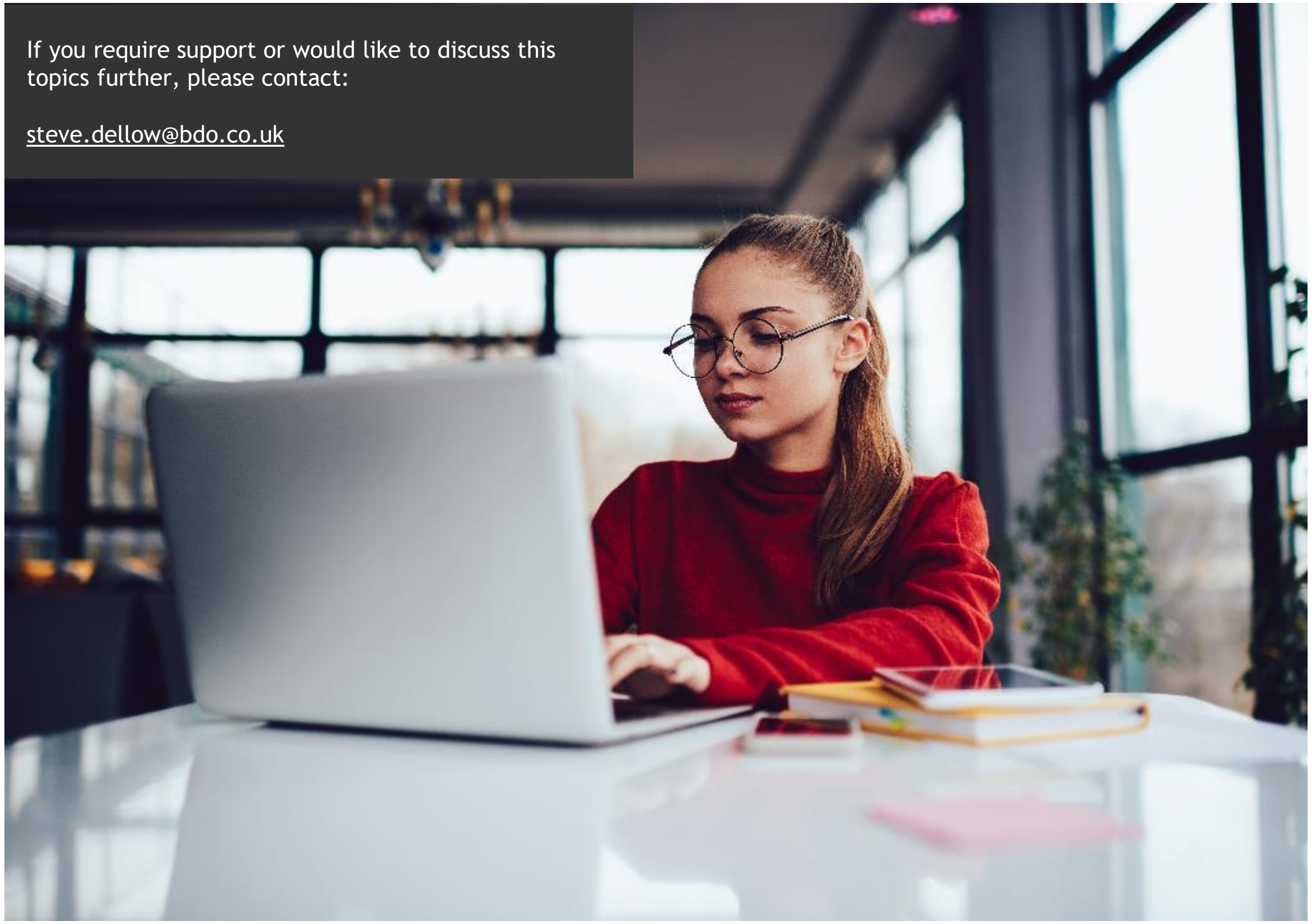
The IIA intends to introduce additional Topical Requirements, encompassing third-party oversight and culture, business resilience, and anti-corruption/bribery. The Third-Party Topical Requirement has been already issued for public review, whereas the culture, business resilience, and anti-corruption/bribery requirements are slated to be drafted during 2025 or 2026.

What this means for firms

For firms, the new Cybersecurity Topical Requirement means a more structured approach to evaluating cybersecurity processes and controls. While it’s aimed at encouraging internal auditors to enhance their cybersecurity knowledge, firms will also benefit from clearer expectations and improved risk management. As more Topical Requirements are introduced, firms can expect further guidance on specialist areas.

If you require support or would like to discuss this topics further, please contact:

steve.dellow@bdo.co.uk



Driving quality in internal auditing: Harnessing the power of External Quality Assessments (EQA)

External Quality Assessments (EQA) enhance Internal Audit (IA) functions in terms of the quality of their outputs and overall performance. Changes brought in by the new Standards and Code, effective from January 2025, emphasise the importance of quality. EQAs provide opportunities to align with industry benchmarks, strengthen stakeholder trust, and transform IA functions into leaders in quality and organisational success. Despite the benefits, many firms have not conducted EQAs, missing opportunities to drive enhancements to their audit processes, outputs and overall performance.

Bruk Woldegabreil
Director, FS Advisory

bruk.woldegabreil@bdo.co.uk

Aditi Kochhar
Manager, FS Advisory

aditi.kochhar@bdo.co.uk

Sam Ewen
Manager, FS Advisory

sam.ewen@bdo.co.uk

Quality, the degree to which a product or process meets its expectations, is rightly a key area of focus for internal auditors. The IIA, through its new Global Internal Audit Standards (Standards), effective since 9 January 2025, reaffirmed the importance of an effective Quality Assurance and Improvement Programme (QAIP), regular self-assessments, and an external quality assessment (EQA) every five years to ensure the internal audit (IA) function maintains high quality. In addition, the new Standards mention quality 126 times compared to just 18 in the IPPF version from 2017, highlighting the growing importance of quality management within Internal Audit in driving trust and credibility with the Board and Senior Management.

Quality assessments, whether through an EQA or a self-assessment with independent validation from an advisor, can help an IA function reflect on the most meaningful aspects of its work (e.g., depth of annual planning) and the perception of IA held by its key stakeholders, i.e., Audit Committee (AC), Board and the Executive.

Despite this, the 2024 CIIA Internal Audit Benchmarking Report, found that just over a fifth of firms surveyed had not conducted an EQA or externally validated self-assessment for their IA function in the last five years. Among smaller internal audit teams of ten or fewer, 27% had not undergone an assessment, whereas all teams with 50 or more members had completed an external self-assessment.

While this is an improvement on previous results, it suggests that small to mid-sized firms may be missing the opportunity to review and enhance their audit processes with professional support and improve the overall performance of the third line through an EQA or self-assessment with independent validation.

During April - September 2023, we published our five-part ‘Quality Matters’ series, which provided a detailed overview of the EQA process, common issues identified through our EQA work, and topical guidance on areas such as IA governance, stakeholder engagement and producing and managing an effective QAIP.

In this article, we provide a fresh perspective on the topic in light of the new Standards and the CIIA’s Code of Practice to explain the benefits of periodic EQAs, what they involve and an overview of some common themes emerging from our most recent work across the financial services sector.

continued >

Back to contents

Driving quality in internal auditing: Harnessing the power of External Quality Assessments (EQA)

Why have an EQA?

An EQA is a requirement under the Standards (Standard 8.4). The Head of Internal Audit (HoIA) must develop a plan for an EQA and the discuss the plan with the Board; within the new Standards, a self-assessment of the IA function with an independent validation can also meet this requirement.

When conducted by a qualified independent assessor like BDO, an EQA goes beyond a simple compliance checklist to assess the function against the Standards and Code requirements. An effective EQA report should offer relevant insights, observations, and benchmarking to help the IA function enhance its effectiveness and add value to the HoIA. An independent assessor confirming the conformance of the IA function to globally recognised benchmarks, the IA function can reassure stakeholders of its ability to deliver reliable and valuable insights, strengthening trust and credibility in its work.

The BDO FS Internal Audit Consulting practice is well-positioned to provide these insights, thanks to the extensive experience gained from working with clients across the FS sector in the UK and globally. This includes expertise in the insurance, banking, payments, and wealth and asset management sub-sectors.

What does an EQA involve?

To prepare for an EQA, the HoIA should engage with the AC and executive management to secure the budget and discuss the scope for a meaningful evaluation of the function.

While the AC Chair should oversee and approve the appointment of the independent assessor, the HoIA is responsible for planning and driving this process at least every five years, as outlined in Standard 8.4. Once successful, a tender process should begin to select qualified and independent assessors. The HoIA should encourage board oversight in the appointment and assessment process to mitigate any potential conflicts of interest.

After appointing an assessor, the EQA assessor will engage with the IA function by reviewing previous EQA outputs, if available, and key documents, such as IA policies and procedures. As the new Standards operate on a ‘comply or explain’ basis, the assessor would also seek to clarify any aspects of the requirements which have been agreed for non-conformance with the AC and the associated rationale. One-on-one interviews would be conducted with senior stakeholders, e.g., INEDs, CEO, CRO, CFO, COO etc, to understand how IA is perceived in the firm. Lastly, a sample of audit files will be selected to assess whether the team have followed established processes, such as around scoping considerations, and the risk assessment.

The assessment will conclude formally on whether the function is Generally Conforming, Partially Conforming, or Not Conforming to the Standards and Code. It will also include recommended remedial actions for any identified vulnerabilities and opportunities for further enhancement, as well as benchmarking analysis to gauge where IA sits alongside comparable peers on a number of key metrics.

What are some common themes from our recent work?

1) IA Strategy

The new Standards require the HoIA to develop a strategy for the IA function which includes a vision, strategic objectives, and supporting initiatives. Our work has identified common themes around strategy and vision, and a common misconception is treating the IA charter as the function’s strategy. While the charter is crucial for establishing the function’s position in the firm and its authority to access records, personnel, and physical assets, it’s not a strategic document. The IA strategy, however, focuses on what the function aims to achieve now and in the future, and what actions are needed to reach those goals. It should also align with the firm’s mission, vision, and actions, ensuring priority risks are addressed and organisational value is enhanced. The most important step in developing an IA strategy is to consult a wide variety of stakeholders to help incorporate the expectations of senior management, the Board and heads of business teams.

2) Independence

Independence is critical to an IA function’s mission and should be actively maintained beyond being documented in the IA charter. Effective IA functions address independence both at the organisational and individual level, ensuring that auditors, especially those long-tenured, are periodically assessed for potential impairments.

continued >

Back to contents

Driving quality in internal auditing: Harnessing the power of External Quality Assessments (EQA)

Risks to independence can gradually develop if not regularly checked, and successful IA functions rotate audits among team members to mitigate familiarity with business areas and document independence through semi-annual assessments or engagement-specific workbooks.

A cohesive combined assurance approach is crucial to define the scope of IA's activities, clarifying each assurance provider's responsibilities and where IA's input is expected by the AC. While assurance planning between IA, second-, and first-line teams is common, it's not always documented in a single location. We will often recommend that functions routinely reassess the combined assurance approach to bring them in line with changes to the IA strategy, annual audit plan, any recent internal reorganisation, and to ensure they are sufficiently visible to senior management. It's not easy, but there should, at minimum, be good communication and collaborative effort taking place between second and third line to avoid duplicative work and mixed messages to the Board.

3) Annual planning

Effective IA planning hinges on a comprehensive audit universe, incorporating inputs like the firm's strategic plan, risk management framework, and regulatory requirements. However, we sometimes find the auditable areas within the universe are outdated, failing to keep pace with regulatory changes or business developments. This can leave firms exposed to significant risks, such as insufficient audit coverage of operational resilience controls.

Regular reassessment of risks and feedback from senior management should be part of the planning process, as outlined in Standard 9.4. An obsolete audit universe can also lead to the AC being unaware of areas not reviewed in some time (e.g., more than 2 years), hampering its ability to challenge the executive management effectively.

We have also found that insufficient audit planning is often highlighted though the absence of thematic or end-to-end reviews. Thematic reviews address cross-cutting themes like culture, while end-to-end reviews cover processes spanning multiple functions, such as operational resilience and claims management. Cyclical reviews should cover areas expected by regulators, such as liquidity and corporate governance, to ensure oversight of recurring key risks. Resource limitations can also lead to audit plans being driven by the skillsets available in the IA team rather than key risks, impacting audit's overall effectiveness. In such cases, we would recommend that the HoIA communicate resource constraints to the AC, to explore options for external support to deliver critical parts of the plan, as per Standard 8.2.

4) Engagement planning

Turning from annual planning to engagement planning, EQAs often reveal that the technical skills and resources needed for assurance over complex subjects or business areas are underestimated. A typical example is a cyber review, which might be allocated ten days by the HoIA. However, given the complexity of information systems, a more realistic timeframe could be 30 to 40 days, especially if coordinated with a cosource provider. The ten-day review may be completed, and a report presented to the AC stating cyber has been covered. However, the AC may lack the context to understand the scope of the review, including exclusions and the limited testing possible within such a short period (Digital Director Steve Dellow has noted the complexity of these requirements in the previous article). It's worthwhile highlighting that securing sufficient specialist resourcing is crucial, especially with the CIIA's updated Code in mind. New specialist risk areas covered in the critical scope areas include financial crime, economic crime and fraud, and technology, cyber, digital, and data (see Principle 8).

5) Open and overdue actions

The new Standards add requirements around corrective actions, including for IA to identify specific owners and target completion dates, and acknowledge actions initiated or completed during the engagement. Within our EQA experience, we have observed that most IA teams are proactive in addressing open issues, ensuring resources are allocated to resolve them promptly. However, when actions remain open, they often become severely overdue due to factors like repeatedly extended due dates, which can cause the AC to lose track of the initial issue raised by the HoIA. Often, big issues remain open while waiting for strategic solutions that may take years to implement.

continued >

Driving quality in internal auditing: Harnessing the power of External Quality Assessments (EQA)

A pragmatic approach is to focus on short-term tactical fixes in the meantime. For example, while strategic solutions for user access controls are ideal, detective solutions like scheduled checks can mitigate risks in the interim. Furthermore, the firm's culture can impact progress on open actions, with limited challenge from the AC potentially indicating broader cultural issues. This lack of challenge may result in key risks not being adequately addressed due to boardroom politics or deference to income generators. Such cultural dynamics can hinder efficient progress on resolving open actions, leaving the firm vulnerable to risks that remain unaddressed in legacy reviews.

Conclusion

An EQA presents a strategic opportunity to enhance audit processes, align with industry benchmarks, and strengthen stakeholder trust and confidence in IA's assurance activity. Regular assessments ensure that IA functions are not only compliant, but also leaders in quality, improving IA's reputation within the firm and standing among peers in the market. The introduction of new the Standards and Code serves as a timely reminder to consider an EQA if one hasn't been conducted in the last five years. By embracing the insights, improvements offered through EQAs, firms can transform their IA functions into pivotal drivers of quality, impacting not just IA but the entire firm.

If you require support or would like to discuss with any of these topics, please contact:

bruk.woldegabreil@bdo.co.uk or
Aditi.Kochhar@bdo.co.uk

Back to contents

Confronting non-financial misconduct in financial services

Beyond breaches of regulatory compliance and financial impropriety, the culture of firms, and behaviours of individuals within them, is now recognised as a fundamental risk to market integrity, financial success and public trust. Once considered peripheral to financial performance, instances of employee bullying, harassment, discrimination and other forms of unethical conduct are now squarely in the focus of FS regulators, stakeholders and the wider public. This has most recently been highlighted in the FCA's decision to fine and ban Crispin Odey of Odey Asset Management LLP from the UK financial services for a lack of integrity (FCA, 2025).

Sasha Molodtsov
Partner, FS Advisory

sasha.molodtsov@bdo.co.uk

Jennifer Cafferky
Associate Director, FS Advisory

jennifer.cafferky@bdo.co.uk

The golden thread

Culture is not a new topic for the FCA, and most firms will be familiar with the FCA's four "drivers of culture": purpose, leadership, approach to rewarding and managing people, and governance. The FCA believes that NFM is one measure of a firm's culture and is therefore relevant to the assessment of a firm's ability to operate in line with regulatory standards. A poor culture is more likely to be complicit in enabling poor decision making and/or permitting activities that breach regulatory standards such as NFM.

Culture refers to the shared values, beliefs and ways of working that characterise a firm (CIPD, 2024), and these characteristics can give us an insight into the sort of conduct and decision-making we might expect. In firms where good conduct and strong decision-making is embedded in its culture, acts of bullying, harassment and discrimination are simply not tolerated. Not only are systems and controls effectively operating, but employees and leaders do not condone these actions, and management has a pulse on not only readily monitoring and detecting instances, but proactively reducing the risk of incidents occurring.

Business leaders should feel empowered to mould and enhance conduct and discourage the sort of conduct which brings risk to their business. In her February 2025 speech, "Culture is contagious", Emily Shepperd, Chief Operating Officer at the FCA stated that "one of the clearest warning signs of a failing culture is NFM" (10th Annual Culture and Conduct in Financial Services Summit).

Addressing NFM is a strong signal that firms are taking action to promote good market outcomes and reduce harm to consumers.

Each firm's culture is unique. Leaders must ask themselves: *what sort of conduct do we want our culture to encourage? Does our culture enable us to achieve our strategic goals, guardrail behaviours in line with risk appetite, ensure consumer duty and protection, drive productivity, and ultimately, contribute to the bottom line.*

UK regulatory landscape

NFM has emerged as a critical issue both within and outside the Financial Services sector and is reflected in the 2024/25 regulatory agenda. Key developments which will impact the Financial Services industry include:

- UK legal updates delivered in October 2024, including the Employment Rights Bill, which prioritises fairness, equality, and worker wellbeing, the Equality (Race and Disability) Bill, which proposes consultations on ethnicity and disability pay gap reports, and the Worker Protection Act which introduced a mandatory duty on employers to prevent sexual harassment (see our article on The New Worker Protection Act & sexual harassment in the workplace)

continued >

Back to contents

Confronting non-financial misconduct in financial services

- The results of the FCA's NFM Survey (published October 2024) surveyed London market insurers and intermediaries, wholesale banks and brokers, and provided unparalleled insight into the sector prevalence of NFM and key focus areas, including prioritising speak-up cultures, whistleblowing channel, sophisticated management MI, governance, and prevention and escalation systems and controls
- Lloyd's updated its Culture Principle in July 2024 to encourage the embedding of inclusive practices in the market. This includes fostering inclusive behaviour with zero tolerance for inappropriate conduct and encouraging psychological safety to promote speaking up. Furthering this focus, in September 2024, Lloyd's launched a consultation on proposed changes to its conduct framework intended to 'modernise' its approach to dealing with both financial and NFM of its members.

What to expect in 2025

The FCA has prioritised the NFM regulatory agenda, indicating potential areas for action and informing the market to expect final rules in this area in June 2025. The FCA's proposals focused on three key areas, which are expected to be included in the regulatory guidance:

1. **Conduct Rules (COCON)**: These apply to most employees in Financial Service firms and are proposed to be amended to explicitly reference NFM, such as serious instances of bullying, harassment and similar behaviours.

2. **Fitness and Propriety Tests for Employees and Senior Personnel:** Proposition to amend the FIT handbook to include NFM in Fit and Proper assessments for employees and senior personnel. This may extend to an individual's personal or private life behaviour, to assess if an individual performing senior management functions or certification functions are 'fit and proper' to hold their role, with potential implications for regulatory references.

3. **Suitability Guidance on Threshold Conditions:** Suitability criteria for firms to include offences related to demographic characteristics and discriminatory practices, giving firms reassurance needed to take decisive and appropriate action against employees for instances of NFM.

How can you prepare?

Preparing for the NFM regulation in isolation and failing proactively consider a holistic picture of your firm's culture is a missed opportunity for leaders. Understanding, measuring and monitoring your culture is vital for the upcoming regulatory change and the health of your firm.

In preparing for these changes, leaders should consider:

- Understanding your firm's unique risk profile and regulatory requirements
- Conducting culture assessments and internal investigations to understand the current state of your firm's culture to determine systemic issues
- Whether your firm's leaders recognise their roles in culture definition, reinforcement and monitoring
- Whether controls and systems are defined and operating effectively. This goes beyond having Policies and Procedures that cover whistleblowing and NFM. These must include clear guidelines for acceptable behaviour, communicated effectively to employees, ensuring these are embedded into your firm
- Are reporting mechanisms in place, and appropriate awareness and training around those?
- Embeddedness of speak up culture. Are employees encouraged to report misconduct without fear of retaliation? How embedded is your speak up culture?
- The mechanisms you have in place to monitor and evaluate your culture. Sadly, culture is not a once and done implementation. Culture must be continuously and proactively assessed and monitored by leaders in order to 'stay on path'. This means ensuring you have defined the right metrics for your firm, regularly reporting and escalating these to leadership forums in MI and developing proactive action plans to understand and mitigate risks as they arise.

continued >

Back to contents

Confronting non-financial misconduct in financial services

What this means for firms

The evolving regulatory landscape surrounding NFM in Financial Services places a clear emphasis on culture and governance. Firms must stay informed about these changes and take proactive steps to address misconduct. By fostering a positive culture and implementing robust policies, firms can ensure compliance and build workplaces that value integrity and respect. This not only protects the firm's reputation but also contributes to a healthier and more sustainable Financial Services sector.

BDO is committed to assisting firms in navigating these changes and implementing effective strategies to address NFM. BDO's FS advisory team is ready to support firms in fostering a culture of integrity and respect, ensuring they thrive in this evolving landscape.

If you require support or would like to discuss this topics further, please contact:

sasha.Molodtsov@bdo.co.uk or
jennifer.cafferky@bdo.co.uk

Navigating the future: Embracing change in risk management

The financial services sector is at a crossroads and experiencing changes that require firms to shift their approach to risk management. To safeguard operations, achieve commercial success, and deliver exceptional customer experiences, firms need to adapt to technological advancements and regulatory updates. In an ever-changing risk landscape firms must adopt agile risk management practices to stay relevant and competitive in a volatile market.

Sarah Collins
Director, FS Advisory

sarah.collins@bdo.co.uk

Staying Relevant in a Volatile Market

Financial markets are increasingly volatile, influenced by global events, economic shifts, and rising geopolitical tensions. In order to manage these risks and external threats effectively firms need agile risk management processes to respond swiftly to market changes and protect their investments. This agility is crucial for staying relevant, thriving, and surviving in today's competitive environment.

Areas firms should focus on

Competitive Edge through Risk Management

In a sector where competition is fierce, effective risk management can provide a significant advantage. By innovating and offering new products while managing potential risks, firms can secure market share and client loyalty. This strategic approach to risk management is essential for maintaining a competitive edge.

Navigating Business Model Disruption

Innovation is both a benefit and a risk. AI-driven personalisation and the expansion of Open Banking are transforming customer solutions, while decentralised finance platforms could challenge traditional banking models by providing peer-to-peer lending, borrowing, and trading without intermediaries. Managing these risks is crucial for leveraging innovation without compromising stability.

Meeting Customer Expectations

Customers demand robust risk management practices that safeguard their money and investments. Transparency is key to maintaining trust and delivering a quality customer experience. Adapting risk management strategies to meet these expectations is essential for long-term success.

Adapting to the Regulatory Landscape

Regulations are constantly evolving, with authorities like the FCA and PRA introducing new requirements. Firms must adapt their risk management practices to comply with these standards and avoid penalties. Staying ahead of regulatory changes is vital for ensuring stability and transparency.

Harnessing Technology Advancements

The rapid pace of technological change presents both opportunities and risks. Cybersecurity threats, data breaches, and the integration of new technologies require firms to update their risk management strategies. Protecting assets and customer information is paramount in this digital age.

Evolving the Three Lines of Defence Model

The Three Lines of Defence model remains a cornerstone in financial services, providing a structured framework for risk oversight and accountability. Each line plays a distinct role in managing risk, independently reviewing those risks, coordinating and collaborating between the three lines, and an adaptable framework which can respond to the changing risk landscape and needs of the organisation.

continued >

Navigating the future: Embracing change in risk management

Evolving the lines of defence

First Line: The Risk Navigators

Traditionally focused on operational management, the first line is evolving to embrace cross-functional collaboration and new technologies. Digital tools streamline processes, while better-than-ever training and development equip teams to handle future curveballs.

Key Strategies

- AI and Predictive Modelling: Utilising AI for predictive modelling enhances risk forecasting, while streamlining routine tasks like data collection and reporting boosts process efficiency
- Compliance Automation: Automating compliance processes helps teams stay current with fast-changing regulations, reducing non-compliance risks
- Cloud-Based Solutions: These provide scalable risk management tools accessible from anywhere, ensuring flexibility and adaptability
- Specialist Risk Training: Expanding specialist risk training to broader populations within the first line, traditionally limited to second line teams or designated specialists, enhances overall capability
- Future-Focused Practical Learning: Leveraging potential scenarios for real-world challenges prepares teams for unprecedented situations
- Collaborative Learning: Encouraging cross-functional team collaboration aids in sharing perspectives, breaking down siloes, and fostering a culture of shared responsibility.

Second Line: The Risk Strategists

The second line is expanding its role, moving towards strategic involvement in risk strategy and policy development. By leveraging AI and real-time monitoring, these teams enhance their ability to track and mitigate risks effectively. The volatile and fast-changing business environment demands a dynamic approach, with risk teams collaborating closely with operational management. As the focus shifts towards reducing regulatory burdens to boost UK financial market growth, the second line will no doubt evolve further.

Key Strategies

- AI-Driven Risk Assessment: Automating risk assessments with AI for faster, more accurate results, identifying patterns and anomalies that signal emerging risks
- Real-Time Risk Monitoring: Using real-time systems to track risks as they develop, allowing for immediate strategy adjustments to mitigate impacts
- Enhanced Collaboration: Second line teams are increasingly using collaborative platforms to improve communication and coordination with first line teams, so that risk management efforts are aligned.

Third Line: The Risk Guardians

Internal Audit teams are adopting a forward-looking stance, focusing on proactive assessments and continuous auditing. By collaborating with risk management teams, this helps support a cohesive approach to risk management.

Key strategies

- Risk-Based Audits: Focused assessments prioritise audits based on risk levels, directing resources to the most critical issues
- Data Analytics: Utilising data analytics to identify trends and anomalies, revealing control weaknesses and emerging risks
- Continuous Auditing: Shifting to ongoing audits for real-time insights and quicker responses to control issues
- Collaborative Approach: Working closely with risk management teams to align audit findings with risk strategies
- Agile Auditing: Adopting flexible and adaptive audit processes to swiftly respond to changes in the risk environment
- Clear Reporting: Providing clearer, actionable reports to help management make informed decisions to strengthen controls.

continued >

Navigating the future: Embracing change in risk management

Integration and Collaboration Across the Three Lines

Effective risk management requires communication and cooperation across the organisation. Integrated frameworks enable a holistic view of risk, while maintaining the independence of assurance functions through defined responsibilities and robust governance practices.

The Future of Risk Management

Technology is a catalyst for change, enhancing the ability to monitor, assess, and respond to risks in real-time. As digital tools and platforms evolve, risk management will become increasingly embedded into everyday operations. The FCA and PRA's data-led and technology-enabled approach to supervision will nudge 'lagging' firms to innovate further.

Ethics and morality will be at the heart of new risk management practices, so that outcomes remain good and fair for all stakeholders (customer, business, environmental, and other). By fostering a culture of risk awareness, enhancing collaboration, and embracing technology, the sector will be better equipped to manage risks and deliver on strategic objectives.

In summary, the future of risk management is agile, responsive, and deeply intertwined with technological advancements. As the landscape continues to evolve, the Three Lines of Defence model will no doubt adapt to protect the industry's future.

What this means for firms

In a volatile market, firms need agile risk management to stay relevant and competitive. Effective risk management helps navigate business model disruptions, meet customer expectations, and adapt to regulatory changes. The Three Lines of Defence model continues to be the bedrock of effective risk management, with each line playing a distinct role in managing risk. Firms should be asking themselves how they integrate and collaborate across these three lines. And importantly, how can they embrace technology to future-proof their risk management practices.

If you require support or would like to discuss this topics further, please contact:

sarah.collins@bdo.co.uk

Anti-Greenwashing Rule: A year of transparency and accountability?

31 May 2025, will commemorate a year since the introduction of the Financial Conduct Authority's ("FCA") Anti-Greenwashing Rule ("AGR"), aimed at curbing misleading environmental claims by any firm in the financial services industry. This set of rules is part of the wider Sustainability Disclosure Regulations ("SDR") and Naming and Labelling Regime, designed to help consumers navigate the sustainable finance landscape.

Gloria Perez-Torres
Associate Director, FS Advisory

gloria.pereztorres@bdo.co.uk

Anandita A
Manager, FS Advisory

anandita.a@bdo.co.uk

What is the Anti-Greenwashing Rule?
Greenwashing occurs when companies make misleading claims about their environmental practices or products. The FCA aims to tackle greenwashing with these new rules, ensuring firms provide clear, accurate information about their sustainability efforts. This will help consumers make informed decisions and trust the claims made by companies. By setting these standards, the FCA seeks also to promote genuine environmental responsibility in the market.

In essence, this rule means that any firm making sustainability or ESG-related claims must ensure that these claims are:

- Correct and capable of being substantiated
- Clear and presented in a way that can be understood by the consumers
- Complete i.e. firms should not omit or hide important information and should consider the full lifecycle of the product or service
- Comparable by being fair and meaningful in relation to any comparisons to other similar products or services being offered in the market.

These rules have brought about a new way of thinking for financial services businesses in the UK. The impact has been seen primarily in the following areas:

1. Increased Scrutiny: The FCA is increasing its scrutiny of firms' environmental claims. It actively monitors compliance and provides guidance to help firms understand their obligations.

2. Enhanced Transparency: Firms are encouraged to provide detailed reports on their environmental impact, products and/or claims, fostering transparency and trust.

3. Shift in Marketing Strategies: With the risk of penalties for false claims, there is enhanced awareness that marketing strategies must be based on verifiable sustainability efforts and evidence. A firm's services and products should do what they say, and all claims should be supported with robust and credible evidence.

As we mark the one-year milestone, it's crucial to assess how these regulations have reshaped corporate practices.

continued >

Anti-Greenwashing Rule: A year of transparency and accountability?

What has actually happened in the last 12 months?

Throughout the last 12 months of the AGR being formalised and implemented, we have seen waves of actions taken by firms, re-assessing how 'green' their business is. Over the past year, firms have closely examined their environmental credentials. They have meticulously worked to ensure all their claims are free of any potential greenwashing in their marketing materials, products, and disclosures.

Firms responded swiftly to the regulation in spring 2024, taking actions such as:

1. Reviewed their sustainable finance product inventory. Firms quickly assessed how the sustainable finance products were positioned against regulatory and market expectations to ensure that there was no risk of greenwashing posed.

2. Reviewed governance architecture to ensure that policies are in line with regulatory expectations, along with having relevant controls to mitigate, minimise, and manage any greenwashing risk.

3. Assessed the marketing of their products, examined sustainability claims in reports, and set targets related to ESG aspects. These claims may involve goals for sustainable finance and policies that support the transition to a lower carbon economy, evidencing how the firm is working to achieve the goals same. In a few instances, banks have been called out by research organisations for having actions contrary to their policies, such as supporting coal explorations while committing to net zero transition.

While these efforts began in spring and summer 2024, the market still saw firms being criticised for misleading claims through the way products were marketed. Recently, a large UK based bank was criticised for the public-facing nature of its ad due to the lack of detail and information about Bank’s non-green activities.

This is a testament to the ethos of the regulation itself—to ensure that firms make verifiable and evidenced claims. We hope to see that this will help consumers be better equipped to make informed choices, adding a layer of authenticity to claims made by firms on their products and services.

In addition to the above listed steps, to ensure compliance with the AGR, firms will need ongoing processes to integrate the AGR into ‘Business as Usual’ practices as well as within ESG-related policies and risk management frameworks.

What this means for firms

As green products are being increasingly recognised as genuinely linked to sustainable characteristics, their demand is expected to rise. This regulation presents both opportunities and challenges, such as compliance costs to ensure consistency in products sold both in the UK and globally. Firms are now considering the global impact on how information is presented to consumers worldwide.

The EU, along with countries including Australia, Canada, Japan, Singapore and Hong Kong, has been taking steps to ensure consumer protection around greenwashing by adding a layer of responsibility on firms around how they position any public information about products and/or business impact.

One year on, the anti-greenwashing regulations have steered firms successfully towards enhanced transparency and accountability. While challenges persist, the overall impact has been positive, encouraging a more honest and sustainable business environment within the financial services industry. Looking ahead, Internal Audit teams should focus on continued vigilance ensuring the internal controls are redesigned and adjusted to support the business adaptation as this will be key to maintaining this momentum.

Anti-Greenwashing Rule: A year of transparency and accountability?

The role of Internal Audit

As third line of defence, Internal Audit is best positioned to review and assess anti-greenwashing controls including:

1. The AGR risk management framework, policies, procedures and controls, and whether these have been incorporated into daily business activities.

2. The sustainability-related statements in relation to products, services, or business strategy to ensure these are coherent, factually correct and can be substantiated.

3. The governance and oversight controls over the sustainability communications that the firm makes and the extent to which these are being documented and periodically reviewed.

If you need support to understand the anti-greenwashing rule, the SDR regime more broadly, or how BDO can help you, please get in touch with our specialist team.

If you require support or would like to discuss this topics further, please contact:

gloria.pereztorres@bdo.co.uk

02

Banking and Building Societies

Back to contents

Supreme Court judgement: Implications for motor finance and beyond

Motor Finance remains a significant topic for bank and nonbank lenders. The appeal hearing for the three test cases at the Supreme Court concluded in April and a judgment is expected to be delivered in July. **These are important cases and the judgment could have wider implications for firms both within and outside motor finance**. As a result, firm should keep abreast developments and assess the risks and implications for their firms, particularly for financial resilience.

Gareth Miller
Director, FS Advisory

gareth.miller@bdo.co.uk

In the closing minutes of the Supreme Court Appeal hearing on 3 April 2025, we heard that it was "realistic" to expect a judgment in July this year. With the industry is calling for more certainty, a decision sooner rather than later, would be welcome news for firms.

It comes as no surprise that the judgment could have wider ramifications beyond motor finance, as the Supreme Court is considering the broader legal principles concerning the nature of the duties owed by a broker to a customer and the commission paid by a third party. A commission should be fully disclosed and agreed to by the customer, and a significant question is whether the credit broker/consumer relationship (particularly a car sales/credit broker) is the type of relationship that gives rise to these duties. The lender who pays the commission, is responsible due to Consumer Credit legislation, hence why the liability for consumer redress sits with lenders.

Broker/customer relationships are common in the financial sector and the decision could apply to a much wider set of broker/customer relationships. However, not all business, activities, products and relationships fall within the scope of FCA regulation and a potential industry-wide customer redress exercise.

Likely timetable

If the Supreme Court does publish its decision by the end of July, as we anticipate at the time of writing, we can expect an FCA communication by mid-September in response to hopefully bring some much-needed clarity.

The FCA is required to consult to make the rules necessary for a statutory redress scheme, and demonstrate it meets the necessary tests for such a scheme. Consultation is a crucial stage in ensuring questions are raised that can affect the operation and extent of a redress scheme.

An FCA consultation generally runs for three months. Once closed the FCA would consider responses before issuing final rules which are approved by the FCA Board. Potentially it may need to reconsult on some points and repeat the consultation cycle. Potential final redress scheme rules could be published as early as 2026.

Potential FCA consumer redress

The FCA's statement on motor finance review next steps on 11 March 2025 outlined a commitment to consult the sector on a redress scheme within six weeks of the Supreme Court's decision. Any redress scheme will be industrywide meaning it would include all consumers who've sold Discretionary Commission Arrangements (DCAs) and that wider implications for non-DCA motor finance would be assessed pending the outcome of the Supreme Court judgment.

"A redress scheme would be simpler for consumers than bringing a complaint. We would expect fewer consumers to rely on a claims management company, meaning they would keep all of any compensation they receive", the statement outlined.

continued >

Back to contents

Supreme Court judgement: Implications for motor finance and beyond

In effect, this approach would mean all lenders that have sold motor finance via a broker to a customer with a DCA would need to identify all customers and pay a redress amount. The population requiring redress under an industrywide scheme would cover all the effected consumers. The FCA has already determined DCA's are unfair, and therefore a redress exercise is likely.

Claims management companies have been effectively carved out of the redress process by the FCA's announcement. No doubt they will be considering how they approach any FCA consultation and the challenges that could be raised.

Wider implications

If the Supreme Court judgment decides all credit broker/customer arrangements fall within those where duties apply, and commission has not been appropriately disclosed, the FCA consultation would need to determine what happens next to this wider group of consumers. This could mean the redress exercise is much wider, and policy changes to its Handbook are required. For firms, the implications would require a full assessment of exposure.

Potential impacts and steps for firms to take:

Population identification

Practically this presents challenges in ensuring the population of customers is fully identified. This means taking extra steps to identify missing records and information to determine if a customer had a DCA or not.

Redress calculations

A customer's records are also important for assessing redress as the detail may be critical in accurately calculating a redress amount. For example, the interest rates available and charges, repayment history, defaults, or early terminations. The methodology for redress calculations is most likely to be a central feature of any FCA consultation. The Supreme Court judgment could impact how redress is calculated, if it is determined that commission should be fully disclosed and agreed to by the customer in addition to discretion to increase interest rates. Modelling potential scenarios helps to assess potential exposures.

Financial Resilience

As you'd expect, the Supreme Court judgment will play a critical role determining the extent of redress liabilities lenders may face. Modelling scenarios in advance will help firms plan and prepare, and we encourage firms to undertake this exercise. Also, there is the potential for wind down to be reviewed. Regulated firms are required to consider adequate provisions for consumer redress and associated financial reporting.

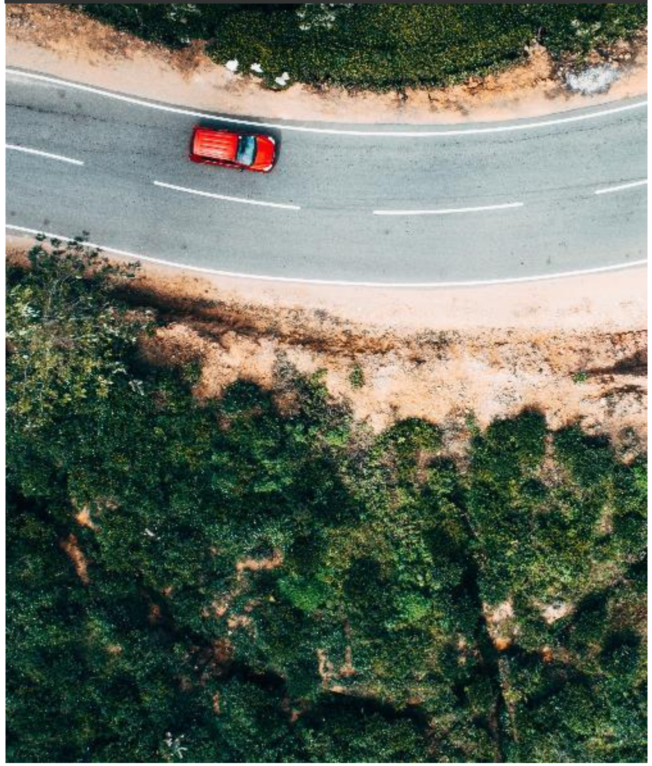
Internal Audit and Risk implications

Firms, and in particular, Internal Audit and Risk function teams should be keeping up with developments and assess the risks and implications, particularly for financial resilience.

More insights are available on our Motor Finance hub.

If you require support or would like to discuss this topics further, please contact:

gareth.miller@bdo.co.uk



Back to contents

PRA proposes new climate risk management expectations for banks and insurers

The Prudential Regulatory Authority (PRA) has released CP10/25, a consultation paper outlining new supervisory expectations for banks and insurers to manage climate-related risks. These proposals aim to help firms address the impacts of climate change, such as severe weather events and long-term effects like sea level rise, which are increasingly affecting their operations.

Gloria Perez-Torres
Associate Director, FS Advisory

gloria.pereztorres@bdo.co.uk

The proposals in this Consultation Paper (CP) consolidates the volume of existing published PRA guidance, embedding improved understanding of climate-related risks and reflect new international guidance that have been issued since 2019. Further, the consolidated proposals respond to the request for more detail on the expectations for firms and highlights that more action from firms will be required to meet the updated expectations.

The PRA's updated expectations focus on enhancing risk management capabilities, ensuring firms can make informed strategic decisions and more clearly incorporate climate-related risk considerations across the business.

According to the PRA, firms have made progress since the initial climate-related expectations in the Supervisory Statement (SS) 3/19 in 2019, but the pace has been slow. The new proposals seek to provide clearer guidance, reflecting lessons learned both domestically and internationally. They emphasise effective risk management practices rather than strict rules, allowing firms to develop proportionate solutions tailored to their business needs.

What is new?

1. The PRA is asking all firms to adopt a two-step step approach to managing climate-related risks:

Step 1: An effective risk identification and assessment process to determine the material climate-related risks they are exposed to and to understand how these risks will impact business resilience over relevant time horizons (short, medium and long) supported by relevant scenario analysis.

Step 2: Developing a risk management framework that is proportionate to their vulnerability to climate-related risk. Specifically, in the interests of proportionality, firms' risk management response should be scaled to the materiality of the climate-related risks they face.

Firms should already have carried out climate-related risk assessments as this has been a requirement since 2019. Internal Audit teams can carry out reviews of existing risk assessments and take the new guidance as best practice when conducting the reviews, which we're encouraging take place sooner rather than later.

2. New expectations on changes to behaviours
The PRA is expecting firms to adopt a more robust Climate Scenario Analysis (CSA), improved climate-related risk management, and incorporate material climate-related risk into firm strategy via governance structures.

As a result, whilst previously climate risk was considered in firm's investments, investment strategies will now need to more clearly incorporate climate-related risk considerations in line with the set risk appetite. Firms would need to assess investments from a climate-related risk perspective. Assets previously thought to be safe could now be found to be riskier and firms may also consider investing more in assets that provide climate-related opportunities. For example, assets required for the UK's and global net zero transition, such as renewables or green innovation financing.

continued >

PRA proposes new climate risk management expectations for banks and insurers

3. A six-month deadline to review the climate risk framework post final publication
After the final SS is published, firms must review their climate risk frameworks to meet the PRA's updated expectations. They will need to identify areas needing improvement and how they plan to address any gaps identified.

The policy takes effect immediately upon publication, but the PRA has indicated that firms will have six months to transition. The transition permits firms to provide evidence of their internal assessments, gap analyses, action plans, or other steps taken to meet the updated expectation within six months of publication rather than immediately upon publication.

Before the final SS is published, firms should continue to manage climate-related risks according to existing expectations and guidance.

What can Internal Audit teams do?

Banks and insurers will have to effectively integrate climate-related risks into their risk management framework and Internal Audit is best placed to support firms with carrying out a gap analysis against the PRA's updated expectations. At the time of writing, the final statement is expected in the third or fourth quarter of 2025. Whilst the final SS may differ from the guidance we have from April, firms should consider taking early action to be able to demonstrate compliance with the new expectations in the first half of 2026.

Internal Audit can help firms prepare by using the draft proposal and existing guidance to recommend updates to risk management frameworks and strategies. The PRA's four pillars—governance, risk management, scenario analysis, and disclosure—should guide this work.

What's next?

The PRA will engage with industry groups to refine best practices and invites feedback on the proposals. The consultation is open until 30 July 2025, and firms are encouraged to share their views, and any potential impacts on groups protected under the Equality Act 2010.

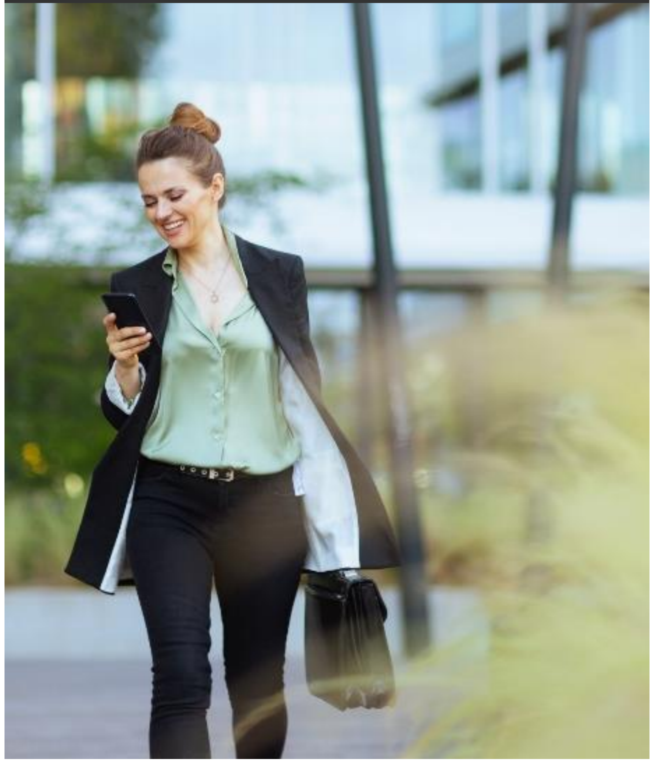
What does this mean for firms?

The message from the PRA is clear and firms must enhance risk management and integrate climate risks strategically. The PRA's detailed guidance signals a commitment to challenging firms on their climate risk management, with enforcement actions possible for non-compliance. Firms should adopt the two-step approach set out above, conduct Climate Scenario Analysis, and align investments with climate risk, with Internal Audit aiding compliance efforts.

The climate change landscape is rapidly evolving despite global political tensions, and firms need to keep pace with these changes. This often requires additional resources and advice. If you have any questions, please contact BDO's ESG Advisory team.

If you require support or would like to discuss this topics further, please contact:

gloria.pereztorres@bdo.co.uk



03

Investment and Wealth Management

Back to contents

Hot topics from FCA supervisors in the wealth sector

We recently met with the FCA Supervisory to better understand the top priorities on their agenda for the Wealth Sector. There are three key messages which we explore more in the article below.

- The Wealth Sector is inherently high risk from a financial crime perspective and the FCA is looking for a significant uplift in financial crime risk management and controls
- Treatment of vulnerable customers is the lens through which supervisors are assessing how well the Consumer Duty is embedded
- Fair Value and pricing outcomes are still under scrutiny. The FCA is asking firms whether pricing offers fair value and good consumer outcomes.

Michael Knight-Robson
Director, FS Advisory

michael.knight-robson@bdo.co.uk

The Wealth Sector is going through a period of change and growth. In 2022, the UK population over 65 was about 12.5 million or 19 % and this is expected to grow to 22.1 million or 27% by 2027 (source ONS). This is leading to an increasing need for personal investment advice and wealth management at the same time as a significant proportion of financial advisers are retiring. Many clients we speak to recognise the need to invest in their businesses with new technology and platforms to increase client service and performance, sometimes with significant investment from PE firms. The UK Government vision for personal finance is to see everyone making the most of their money and pensions. To do this there are a number of strategic initiatives, with FCA supervisory focus on ensuring firms in the sector can deliver good consumer outcomes.

Our conversation with FCA supervisors focused on three key themes that are topics at the top of their agenda for this sector.

Consolidation

Consolidation remains a theme given the amount of activity underway. The FCA has publicly said it is conducting a review of consolidation with a focus on the short and long term client benefits. It has also been reviewing debt servicing, stress testing and financial resilience.

Governance and decision making, particularly where there is consolidation or a growth strategy, need to focus on client outcomes. There is still evidence that decisions are overly focused on the drive for growth.

Decisions about growth also need to take into account the commensurate investment in governance structures and second line resources such as compliance staff. Too often these lag behind resulting in inadequate oversight.

Consolidation can often lead to firms having multiple client fee structures with limited transparency about the fair value of the different prices and fee rates.

Financial Crime

This is a significant risk issue where the view is that this sector doesn't appreciate that it has an elevated risk of facilitating financial crime. Financial crime issues are taking up a large number of supervisory resources. Responses to the FCA's wealth survey are showing weak understanding and assessment of financial crime risks. E.g. 25% of firms submit no annual financial crime checks on high-risk clients. The results also show limited ongoing screening checks or sanctions checks, a lack of knowledge about DAMLs, or consideration of cross border financial crime risks. There are a considerable number of enforcement cases about financial crime related to this sector, including criminal cases. You can see a recent case here.

Fraud and financial crime are two sides of the same coin – one leads to the other, however the FCA sees a lack of investment in fraud prevention and fraud controls.

continued >

Hot topics from FCA supervisors in the wealth sector

Vulnerable Customers

Improvements to the identification and treatment of customers in vulnerable circumstances remains a hot topic. The FCA's recent publications about vulnerable customers provide extensive insights for firms and BDO has also recently published material to help firms navigate improvements to processes. Supervisors are assessing how well consumer duty is embedding through the lens of vulnerable customer treatment. Previous messages published by the FCA have focused on identification of vulnerability and how clients are supported. Recent FCA publications have highlighted a focus on bereavement processes in the banking sector.

Internal Audit teams should consider these topics as part of their risk assessment and audit planning.

If you require support or would like to discuss this topics further, please contact:

michael.knight-robson@bdo.co.uk

Back to contents

A guide to the prudential consolidation rules in MIFIDPRU

On 1 January 2022, the Investment Firms Prudential Regime ("IFPR") came into effect in the UK. The IFPR applies to all firms with FCA permissions to carry out MiFID investment activities and services. The rules and guidance for IFPR are set out in the MIFIDPRU sourcebook of the FCA Handbook. MIFIDPRU includes provisions for the identification of an Investment Firm Group ("IFG") and the regulatory implications of full prudential consolidation or alternative approaches. For firms the considerations since have focussed on what an IFG is, how it is constituted, and the implications for firms' compliance.

For groups with investment firms correctly identifying Investment Firm Groups (IFGs) under the MIFIDPRU consolidation rules is crucial in meeting regulatory obligations.

Osita Egbubine
Associate Director, FS Advisory

osita.egbubine@bdo.co.uk

Who are the MIFIDPRU consolidation rules relevant to?

They are relevant to any group of companies that includes at least one MIFIDPRU investment firm, or anyone planning to acquire such firms or groups.

Why is it important to get the IFG right?

Under the rules in MIFIDPRU, several obligations apply to IFGs, including governance arrangements, risk management, regulatory reporting, capital and liquidity adequacy assessment, remuneration and to some degree, the Internal Capital Adequacy and Risk Assessment ("ICARA"). An unidentified or poorly assessed IFG could lead to breaching these requirements. The FCA has recently expressed concerns about corporate group structures that deliberately or inadvertently hide group risks, which leads to increased scrutiny in change in control or variation of permission applications and supervisory regulatory reporting reviews.

What is an IFG?

An IFG is a group of entities where at least one firm in the group is a MIFIDPRU investment firm (i.e. a UK investment firm in scope of the IFPR). It comprises the firm's UK parent entity and its subsidiaries and connected undertakings. The MIFIDPRU investment firm may or may not be the UK parent entity. MIFIDPRU also introduces the concept of a 'deemed parent'. This will apply where the entities are connected undertakings rather than in a parent/subsidiary relationship.

An IFG may also have a group entity that is a UK credit institution (i.e. a bank), in which case the group will be subject to the consolidation rules under the UK Capital Requirements Regulation ("UK CRR").

What are subsidiaries and connected undertakings?
A subsidiary follows the legal definition set out in s.1162 of the Companies Act 2006 which includes entities in which the parent entity holds or controls the majority of the shareholdings or voting rights, has the right to appoint or remove the majority of the directors of the entity, or has the right to exercise dominant influence over the entity. It also includes subsidiaries of subsidiaries.

Connected undertakings are entities with one of the following relationships:

- **Majority common management** - entities A and B will be connected undertakings if the majority of their boards comprise the same people
- **Significant influence** - this would be the case if one entity has the power to participate in the financial and operating policy decisions of another entity. This consideration is nuanced and should consider the relevant facts and circumstances. Indicators include the power to appoint Board representatives or to decide on the distribution of dividends in another entity

continued >

A guide to the prudential consolidation rules in MIFIDPRU

- **Single management** - two or more entities have effectively coordinated financial and operating policies. This also requires a factual consideration of the relevant facts and circumstances. Indicators include control by the same natural person or group of natural persons over the entities, or concentration into one person of the power to appoint the majority of the Boards of those entities
- **Participation** - a participation is defined as an entity owning 20% or more of the shareholding or voting rights of another entity. A participation may also be present if one entity holds rights in the capital of another entity (even if below 20%) which creates a 'durable link'. A durable link could be established for example if the intention is to increase holdings or influence over another entity over time.

Are all subsidiaries and connected undertakings included within the IFG?

Only those subsidiaries and connected undertakings which are Relevant Financial Undertakings ("RFU") are included as defined below:

- an investment firm (i.e. firms authorised to provide investment services or perform investment activities)
- a non-UK credit institution (i.e. entities with permissions to accept deposits)
- a financial institution (e.g. holding companies, payments or e-money institutions, article 2 or article 3 exempt firms, UCITS management companies or Alternative Investment Fund Managers)
- an ancillary services undertaking (i.e., entities whose principal activity is owning or managing property, managing data processing services or other ancillary activities to the principal activity of investment firms)
- a tied agent (excluding mere appointed representatives).

Note that these entities are considered for inclusion in the IFG regardless of the country of domicile.

What entities are included in the IFG?

Based on the foregoing definitions, the IFG will comprise the MIFIDPRU investment firm, and any RFUs in its group up to the highest UK parent entity, subsidiaries and connected undertakings of the UK parent entity and/or the MIFIDPRU Investment firm. How do prudential requirements apply to an IFG in practice?

An IFG is required to comply with the own funds and liquidity adequacy rules based on its consolidated situation. In other words, an IFG must hold sufficient own funds to meet the consolidated own funds requirements considering the consolidated permanent minimum requirements, consolidated fixed overheads requirements and where applicable, consolidated K-factor requirements. It must also hold sufficient liquid assets to meet its consolidated basic liquid asset requirements. IFGs also must comply with consolidated reporting, concentration risk management and remuneration requirements.
The responsibility for complying with the applicable rules to IFGs typically rests with the UK parent entity, which must ensure that all IFG entities, regardless of jurisdiction and regulatory status, implement the necessary arrangement to enable IFPR compliance.

How does an IFG consolidate subsidiaries and connected undertakings?

Standard accounting principles and practice are followed when consolidating subsidiaries. This includes treatment of intercompany balances and investments in subsidiaries vs share capital. The default position is full consolidation of all subsidiaries that are RFUs. Proportional consolidation can be used in case of Participation. For connected undertaking relationships where there are no capital ties, approaches such as the aggregation method are used.

Can I exclude entities within the corporate group structure from the IFG?

The identification of an IFG is a process that entails some judgment on relationships/connections and interpretation of relevant rules and definitions. As such the prudential consolidation analysis, as well as the exclusion of any group entities from an IFG, must be based on robust regulatory assumptions, supported by relevant facts and circumstances and appropriately reviewed and approved by the Board.

continued >

A guide to the prudential consolidation rules in MIFIDPRU

The FCA will strongly challenge any attempts to avoid the consolidation rules where these apply.

Can overseas entities be included within the IFG?

Where a group includes non-UK entities, these entities could be included within the IFG if they are RFUs in a parent/subsidiary or connected undertaking relationship with the MIFIDPRU firm or the UK parent entity.

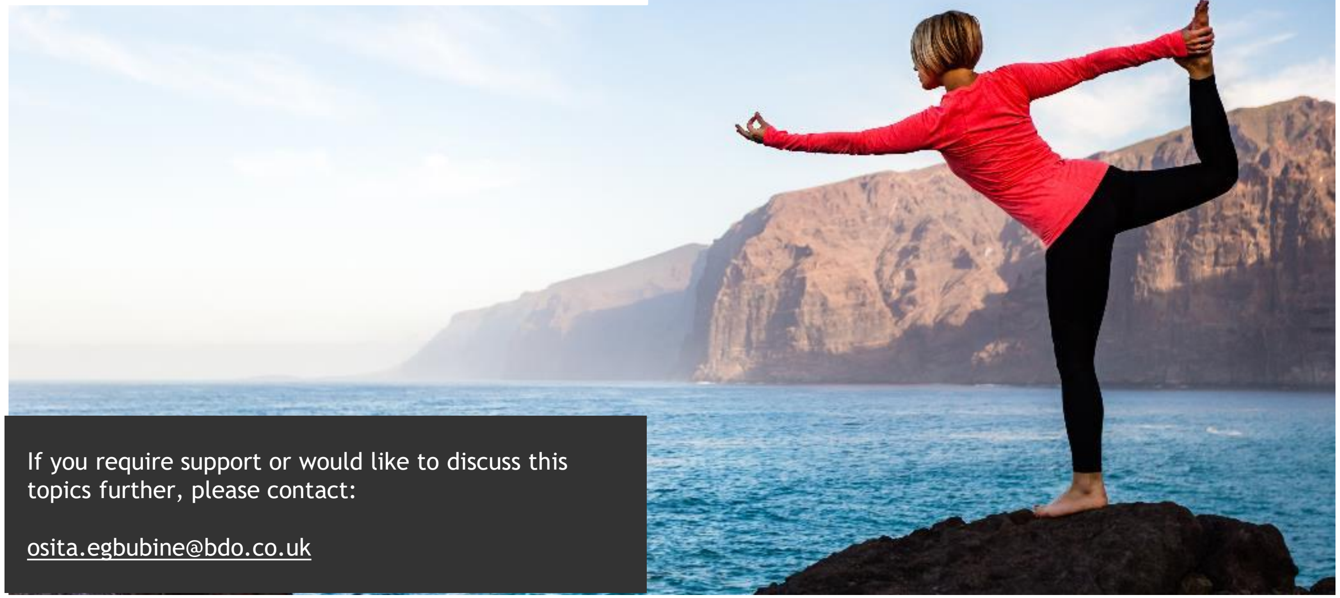
The FCA, in its 2021 technical webinar, confirmed the concept of a 'deemed IFG'. This refers to an IFG where overseas parent entities and/or connected undertakings are attracted in scope of the MIFIDPRU consolidation regime. Careful analysis is therefore required to understand the precise nature of the relationships between group entities and identify the UK parent of the deemed IFG.

If I have identified an IFG, does that mean I need to prepare a consolidated ICARA?

No. The FCA will advise a group if they expect it to prepare a consolidated ICARA, in addition to the individual ICARAs of each MIFIDPRU firm. An IFG may however independently opt for a 'group ICARA' covering all IFG entities.

What does this mean for firms

Investment firms and groups should be confident that they have carried out a robust prudential consolidation analysis to identify all the entities that should be included in the IFG. The basis for the conclusions reached, including any key judgments and assumptions, should be clear and signed off by the appropriate governance forum. Once the constituent entities within the IFG have been identified, the UK parent entity (or the MIFIDPRU firm by delegation) will maintain group governance and oversee the IFG's compliance with all consolidated regulatory requirements.



If you require support or would like to discuss this topics further, please contact:

osita.egbubine@bdo.co.uk

Back to contents

Liquidity risk management: FCA's multi-firm review of wholesale trading firms

In March 2025, the FCA published the results of its multi-firm review of liquidity risk management at wholesale trading firms, mostly brokers in scope of the Investment Firms Prudential Regime ("IFPR").

The findings and feedback provided by the FCA are particularly relevant to commodity clearing brokers, commodities traders, inter-dealer brokers and CFD firms. However, the outcomes are relevant to all investment firms and demonstrate the FCA's increased focus on liquidity risk management in the financial sector.

A robust and effective liquidity risk management framework, including liquidity risk governance, stress testing, contingency funding and effective cashflow monitoring has wide reaching benefits.

Arka Dey
Manager, FS Advisory

arka.dey@bdo.co.uk

The FCA has recently published the results of its multi-firm review of liquidity risk management at twenty-six larger wholesale trading firms in scope of the IFPR. While these are not systemic firms, they operate in commodities, metals and energy markets and provide crucial clearing and settlement services to market participants, posing liquidity and reputational risks, particularly when connected to larger groups.

Significant liquidity challenges

In recent years, the financial landscape has been affected by several stress events, including the COVID pandemic, growing geopolitical tensions and market volatility across the financial services sector.

Over the past two years, the FCA has intensified its supervisory work to address liquidity shocks and monitor how firms manage and mitigate liquidity risk as required in the MIFIDPRU rules. The key expectation is for all firms to maintain effective liquidity risk management processes to identify, quantify, monitor, and address daily risks and financial stress, ensuring they can meet liabilities as they fall due at all times.

Key Findings

Most firms in scope were found to underestimate their exposure to intraday liquidity risks and face challenges from sustained volatility, high prices, substantial margin calls, credit stresses and increased counterparty risks, all of which increase the risk of harm to market integrity.

The FCA's review highlighted some common issues including:

- failure to comprehensively identify and quantify idiosyncratic liquidity risks
- excessive reliance on immediate access to liquidity facilities
- poor management of client relationships and outsourcing arrangements
- lack of clear metrics and triggers in setting liquidity risk appetite
- underestimation of liquid asset threshold requirements ("LATR")
- inoperable contingency funding plans ("CFP")
- weaknesses in liquidity stress testing.

In addition, more specific findings were raised in respect of typical wholesale trading business models. Some firms:

- did not quantify intraday exposures at T0 or estimate the peak exposure for the next day under stress (e.g. margin calls)
- displayed ineffective monitoring of trade and cash flows throughout the day and inability to react promptly to liquidity shortfalls
- lacked of re-assessment of ongoing appropriateness of membership to central counterparties.

continued >

Liquidity risk management: FCA’s multi-firm review of wholesale trading firms

- had stress testing models that did not include behavioural and operational assumptions around margin calls, settlement failures, client facility drawdowns, withdrawal of unsegregated client money, pre-funding requirements and failure to rollover debt
- placed too much reliance on LME’s daily price caps as mitigation for prolonged large price movements
- failed to calibrate and test value at risk (“VaR”) models against changing outflow volumes
- failed to consider potential stresses affecting liquidity providers.

FCA’s Views on Good and Poor Practice

The FCA’s feedback, while specific to sell-side trading firms, includes plenty of helpful examples of good and poor practice that should be taken in due consideration by all firms.

Good Practice:

- Firms with strong governance and risk culture focus on optimising long-term performance and resilience, not just regulatory compliance. They dynamically assess intraday risk exposures daily, ensuring these remain within defined risk tolerances
- They have clear risk appetite limits and action triggers, considering both financial and non-financial criteria. Regular reviews and analysis of risk events support the management of liquidity risk
- As part of stress preparedness, firms are conducting forward-looking stress assessments daily, as is proportional to the level of intraday liquidity risks faced, particularly if significant daily variations arise
- Accurate and effective processes for ongoing cashflow monitoring allow prompt reaction if needed
- Contingency funding plans have clear action triggers and a range of actions to increase or conserve liquidity
- Wind-down plans include detailed cashflow analysis and consider reverse stress testing outputs in the calibration of triggers and thresholds
- Liquidity risk management teams continuously update expertise and frameworks, ensuring a holistic approach that integrates operational processes.

Poor Practice

- Some firms struggle to embed even well-designed frameworks, relying on senior executive sponsorship rather than a strong risk culture across the firm
- Stress testing is often infrequent and fails to reflect actual liquidity outflows, by underestimating number and magnitude of margin calls
- Weakness in the range of stress scenarios and assumptions where these are not realistic and do not capture the full range of liquidity exposures firms may be facing
- CFPs lack clear action triggers and consider only a limited range of available actions, increasing risk during sudden liquidity stress
- Liquidity risk management teams may lack expertise, leading to understated risks and inadequate frameworks
- Outsourcing arrangements are poorly understood, with risks posed by third-party providers not proactively managed
- A box-ticking approach was observed in some firms, which shows insufficient application of regulatory requirements and a lack of a sound liquidity risk management culture.

FCA’s action

Further to the review, the FCA has taken direct action on the firms in scope, depending on the severity of its findings, such as imposing Individual Liquidity Guidance (“ILG”), requesting assurance reports to confirm remediation and providing recommendations for improvement.

continued >

Liquidity risk management: FCA's multi-firm review of wholesale trading firms

The FCA continues to express its expectations around liquidity risk management as set out in the MIFIDPRU rules, its Finalised Guidance 20/1, the results of its previous multi-firm reviews in 2023, its Wind-down Planning Guide ("WDPG") and its Thematic Review 22/1 on wind-down planning, liquidity and intragroup dependencies.

What does this mean for firms

To ensure your liquidity risk management framework remains fit-for-purpose, we recommended that firms adopt a holistic approach to risk management. This involves integrating liquidity risk taxonomy and appetite levels based on direct experiences with internal and external risk events. Even more important is that firms undertake regular assurance reviews conducted by either the risk oversight function or internal audit.

If you require support or would like to discuss this topics further, please contact:

arka.dey@bdo.co.uk

Back to contents

Wealth and asset management sector "too complacent" with its financial crime systems and controls

The FCA has recently highlighted that the wealth and asset management (WAM) sector is "too complacent" with its financial crime systems and controls. Since last year the sector has been under increased attention from the regulator leading them to have concerns, noting gaps in firms' assessments.

A recent roundtable at our London office including several firms revealed fraud is considered the real risk and that they suffer from gaps in data. Compliance functions are also struggling to engage the business on managing financial crime risk.

Michael Knight-Robson
Director, FS Advisory

michael.knight-robson@bdo.co.uk

In the last 10-15 years, the regulator has focused on sectors cyclically. This started with the UK largest banks such as HSBC before scrutinising subsidiaries and branches such as Guaranty Trust Bank. In more recent years Payments and e-Money Institutions have been subject to a wave of s166 or Skilled Person reviews.

In the last 6-9 months, there has been an increase in Skilled Person reports in the WAM sector a number of which we have worked on. Through our engagement with the FCA they have told us that they are now turning their attention to financial crime compliance in the sector, due to it "falling over" weaknesses in recent visits.

What financial crime related issues is the regulator concerned with?

- Firms consider themselves low risk, as they are "not a bank". This is contrary to the UK's Money Laundering and Terrorist Financing Risk Assessment which highlights the sector as high-risk for money laundering
- Firms' financial crime compliance frameworks are not underpinned by a robust financial crime business-wide risk assessment (BWRA)
- Financial crime compliance monitoring and testing (second line of defence assurance over the first line of defence) is limited and not risk-based
- Firms' fraud risk management focusses on external factors with insufficient consideration of internal fraud risks.

Fraud - the real risk

BDO recently hosted a WAM financial crime roundtable to consider the challenges presented by the current regulatory and legislative focus. Fraud emerged as "the real risk" with firms concerned that the Economic Crime and Corporate Transparency Act (ECCTA) Failure to Prevent Fraud corporate criminal offence, which comes into effect from 1 September 2025, will open the door for the FCA to scrutinise firms' internal and external fraud risk management controls. With virtual business replacing face-to-face interactions, impersonation fraud is seen as a key risk. To mitigate this firms are starting to apply biometric ID&V technology.

As BDO highlighted in November, Home Office Guidance gives 6 key principles for 'reasonable procedures'. While specific to ECCTA, (internal fraud risks and firms who meet the 'large' thresholds) firms who fail to apply this approach across all fraud risks, and irrespective of their size, may find themselves subject to attention.

continued >

Back to contents

Wealth and asset management sector “too complacent” with its financial crime systems and controls

The challenge of business-wide risk assessments

BWRAs have been a feature of SYSC long before the implementation of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs 2017), which heightened the requirement for to develop a financial crime compliance framework in line with their financial crime risks. However, firms must still meet FCA expectations, including using data to identify and assess risks. This is particularly prominent in the WAM sector, where firms confess to having ‘poor data’, which means they rely on assessments of ‘apparent’ rather than ‘actual’ risk.

When supporting firms with data driven BWRAs, we start by asking for the availability of structured data for more than 100 key risk indicators (KRIs). These include customer, geographic, products and services, transaction and delivery channel risks, as well as results of first line quality control checks, financial crime compliance monitoring and internal audit findings. Many firms have less than 50% of the KRI data available. We signal this as a key area where firms can improve so they can develop a framework that stands up to the regulatory rigour.

The divide between the first and second line of defence

A common issue we see is the maturity of the lines of defence framework, in particular, an expectation that financial crime risk management is the responsibility of the second line with insufficient input from first line and senior management. A mature risk and controls framework should be owned in the first line with second line oversight and monitoring.

We find senior management fail to understand the importance and engage in the process, and with first line input there is still a culture of “us and them”. This is in tune with our experience of the banking sector where we have worked through the overhaul in responsibility and management of financial crime risk. Most banks now realise the importance of the business taking ownership of key financial crime compliance controls.

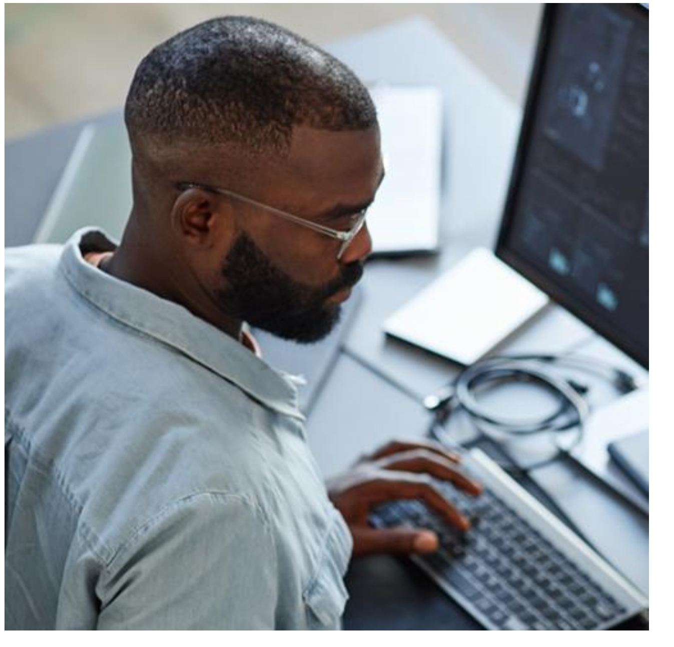
In the WAM sector we have seen key controls still being carried out by the second line of defence, defeating the object of the three-line model which is designed to give firms the best defence. We see firms where compliance teams are conducting controls with minimal oversight and undertaking internal audit review at too low a frequency. WAM compliance teams are typically under resourced and carrying out controls which are more effective if conducted by the first line. This can compromise other areas of compliance including keeping up to date with regulatory expectations and industry best practice.

The WAM sector is playing catch-up with the rest of the financial services industry. Target operating models and roles and responsibilities need to be transformed to give compliance teams, the best chance of success in protecting firms from financial crime.

The key concerns in this article, firms underestimating their risk level, inadequate business-wide risk assessments, limited compliance monitoring, and insufficient internal fraud risk management, are particularly relevant to the WAM sector at the time of writing.

- The Economic Crime and Corporate Transparency Act, which will increase scrutiny on fraud controls, and the recent increase in regulatory scrutiny in this area, serve as a timely reminder for firms to consider the importance of having robust business-wide risk assessments and the need for a mature lines of defence framework, where the first line takes ownership of risk management.

continued >



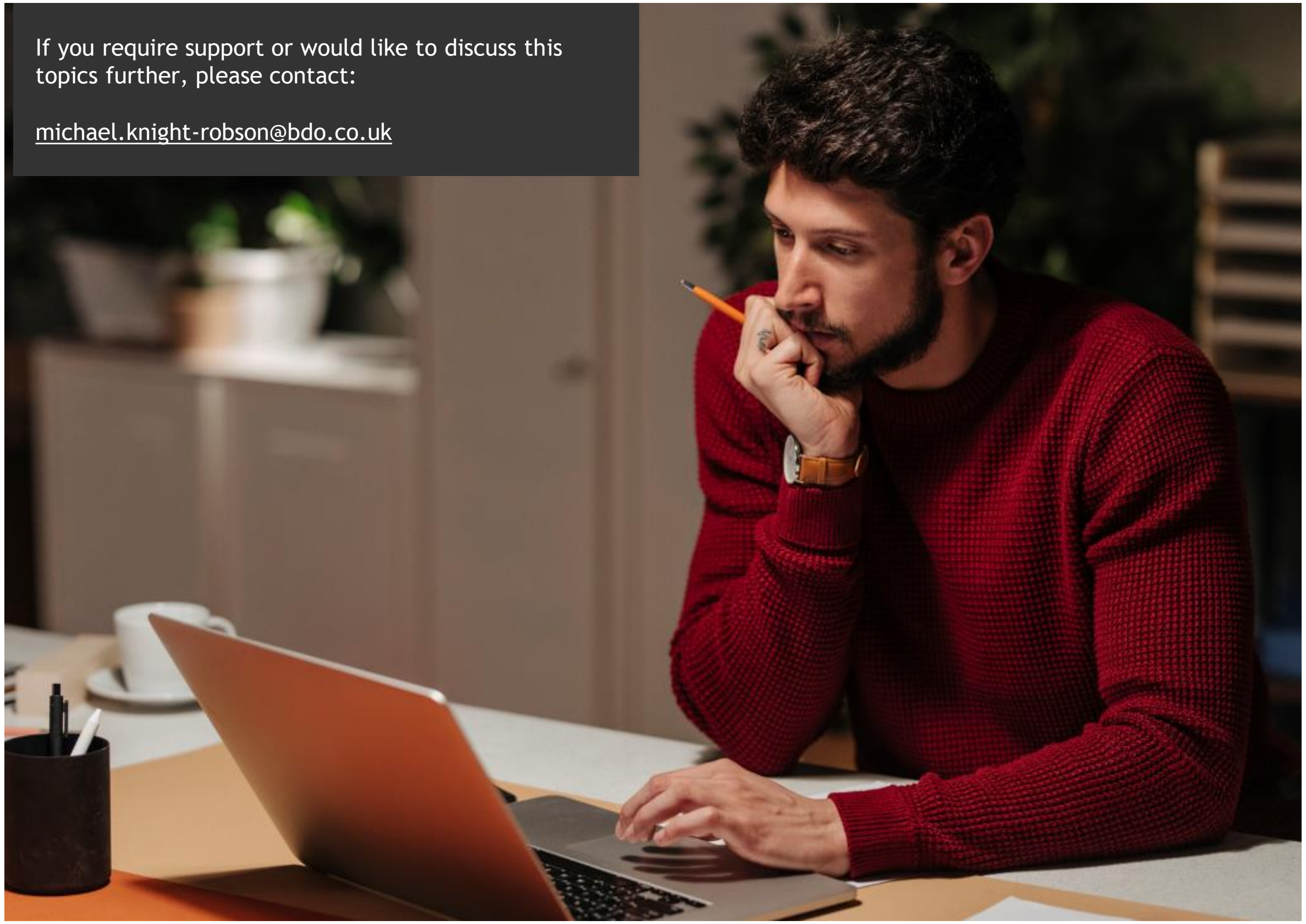
Back to contents

Wealth and asset management sector "too complacent" with its financial crime systems and controls

How BDO has been supporting firms

BDO has a long history of supporting clients within the WAM sector, to help solve complex regulatory issues, to ensure they meet the FCA's expectations. In particular, BDO can support you with:

- Workshops to benchmark how your framework compares to regulatory expectations and industry best-practice
- Independent reviews to assess your framework with practical and proportionate recommendations
- Developing new policies, procedures and risk assessments
- Conducting full-scale framework remediation - from quickly identifying where gaps exist, to uplifting documentation, and then implementing new systems and controls, including conducting backbook remediation of CDD/EDD files
- Delivering training across the three lines of defence, either through e-learning or bespoke tailored face-to-face training.



If you require support or would like to discuss this topics further, please contact:

michael.knight-robson@bdo.co.uk

04

Payments & E-money

Back to contents

FCA Discussion Paper DP25/1: The UK's next steps toward cryptoasset regulation

The UK is accelerating its efforts to build a coherent and robust regulatory framework for cryptoassets. In May 2025, the Financial Conduct Authority (FCA) published Discussion Paper DP25/1: Regulating Cryptoasset Activities, laying the groundwork and discussing key questions to help shape a new, comprehensive regime for firms engaging in crypto-related services.

This discussion paper marks a critical milestone in the UK's phased approach to cryptoasset regulation and provides important insights for payments, e-money, and cryptoasset service providers preparing to operate under full FCA supervision.

Luke Patterson
Partner, FS Advisory

luke.paterson@bdo.co.uk

Zahra Ellahi
Associate Director, FS Advisory

zahra.ellahi@bdo.co.uk

Background: Building the Regulatory Foundations
In 2023, HM Treasury (the Treasury) announced plans to legislate for a dedicated financial regulatory regime for cryptoassets. Until now, regulatory oversight has been limited to:

- Compliance with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs)
- The UK financial promotions regime
- Consumer protection laws such as the Consumer Rights Act 2015 and the Consumer Protection from Unfair Trading Regulations 2008.

In November 2024, the Treasury reaffirmed the previous government's proposals to bring key cryptoasset activities within the Regulated Activities Order (RAO). According to a draft Statutory Instrument, this will introduce regulated activity designations for:

- Operating a cryptoasset trading platform
- Intermediation of cryptoasset transactions
- Cryptoasset lending and borrowing
- Staking services
- Decentralised finance (DeFi) protocols.

These reforms represent the UK's transition toward a risk-sensitive and outcomes-focused regime that aligns with global standards while promoting innovation and financial stability.

Key Themes of DP25/1
The FCA's DP25/1 outlines the regulator's proposed approach for supervising cryptoasset activities and invites industry feedback and specific questions ahead of formal rule-making. Core areas of consultation include:

1. Cryptoasset Trading Platforms (CTPs)
The FCA proposes CTPs be treated similarly to traditional multilateral trading facilities, with obligations around market conduct, operational resilience, trade transparency, and conflict of interest management.

2. Crypto Intermediation
Firms providing crypto brokerage or arranging deals will face conduct rules akin to those for investment firms, including fair treatment of clients and robust risk management.

3. Lending and Borrowing of Cryptoassets
Lending platforms will need to implement strong prudential and disclosure frameworks. This includes protecting client funds, managing counterparty risk, and being transparent about returns and risks.

continued >

FCA Discussion Paper DP25/1: The UK's next steps toward cryptoasset regulation

4. Staking Services
The paper discusses extending the regulatory perimeter to include staking activities, where consumers delegate tokens to validators for network rewards. This could bring staking under client asset and conduct rules.

5. Decentralised Finance (DeFi)
While the FCA acknowledges DeFi's complexity and decentralisation, it signals a future intent to develop an appropriate regulatory perimeter and policy toolkit to address systemic and conduct risks.

6. Use of Credit to Buy Crypto
The FCA raises concerns about the use of credit cards and other financing methods to purchase cryptoassets and is considering intervention to limit consumer harm.

Regulatory roadmap: What's next?

The publication of DP25/1 follows Phase 1 of the UK's crypto regulatory framework, which targeted financial promotions and fiat-backed stablecoins used for payments. Phase 2—now underway—extends the perimeter to a wider set of cryptoasset activities under the Financial Services and Markets Act (FSMA) framework.

Upcoming developments expected in late 2025 and into 2026 include:

- FCA Authorisation Regime for Crypto Firms: All in-scope firms will be required to apply for full authorisation and meet threshold conditions
- Tailored Conduct and Prudential Rules: New standards for governance, capital, client asset protection, and operational resilience
- Market Integrity and Abuse Prevention: Introduction of a bespoke market abuse regime for cryptoassets
- International Harmonisation: Alignment with IOSCO, FSB, and FATF guidance to ensure global regulatory coherence.

Next Steps for Firms

The FCA is accepting responses to DP25/1 until 13 June 2025. Crypto, e-money, and payments firms should take this opportunity to engage with the consultation and begin planning for the coming regulatory changes where they may be impacted.

BDO recommends the following immediate actions:

- Assess your firm's exposure to in-scope crypto activities
- Evaluate systems, controls, and client protection mechanisms against proposed standards
- Prepare for authorisation or variation of permissions under the RAO regime
- Develop internal plans for staking, lending, and DeFi-related services
- Engage in the consultation process to help shape proportional and effective regulation.

How BDO Can Help

BDO's Financial Services Regulatory team supports firms, e-money institutions, and payments companies in navigating regulatory change. We offer:

- Regulatory gap analysis and readiness reviews
- Authorisation support under the FCA's evolving regime
- Governance and risk framework design
- Prudential and conduct compliance assessments.

If you require support or would like to discuss this topics further, please contact:

luke.patterson@bdo.co.uk or zahra.ellahi@bdo.co.uk

PSR/FCA merger - What it means for the payments sector and beyond

The UK government has confirmed that the Payment Systems Regulator (PSR) will be merged into the Financial Conduct Authority (FCA), marking a significant step in the consolidation of regulatory oversight across the UK financial services sector. The merger aims to streamline regulation, reduce duplication, and deliver more effective supervision in an increasingly integrated and fast-moving financial ecosystem.

This development is particularly relevant for payments and e-money firms—but it also has broader implications for banks, consumer credit firms, and any firm reliant on the UK's payment infrastructure.

Luke Patterson
Partner, FS Advisory

luke.paterson@bdo.co.uk

Zahra Ellahi
Associate Director, FS Advisory

zahra.ellahi@bdo.co.uk

The Rationale Behind the Merger

The merger reflects the government's desire to deliver a more agile, coherent regulatory framework that can keep pace with innovation and support long-term competitiveness. The FCA's broader remit, combined with the PSR's technical expertise in payment systems, should provide a more holistic supervisory model for the UK's digital finance sector.

Key Implications for the Payments and E-Money Sector

1. Streamlined Supervision and Reporting
More integrated compliance expectations could reduce regulatory burden, but only after a likely transitional period involving alignment of systems and controls.

2. Greater Scrutiny on Consumer Outcomes
The FCA's Consumer Duty and emphasis on fair value are expected to influence future payment system design, access rules, and dispute handling.

3. Policy Realignment and Innovation Opportunities
Payment firms should be prepared for potential changes in policy direction, especially in areas like access to infrastructure, open banking, and cross-border transaction standards.

Wider Financial Services Market: What to Expect
While the merger is operationally centred on the payments sector, its ripple effects will be felt across the financial services ecosystem:

1. Banks and Building Societies
Banks, especially those involved in payment system governance (e.g., CHAPS, Faster Payments), will face increased oversight over their roles as system operators and indirect access providers. The FCA's approach may result in:

- **Tighter scrutiny of access and fairness** for smaller participants
- **Increased compliance expectations** around systemic resilience and operational risk
- **More direct engagement** with the FCA on issues previously addressed through the PSR, such as scheme fees and infrastructure investment.

continued>

PSR/FCA merger - What it means for the payments sector and beyond

2. Consumer Credit Firms
Although not directly regulated by the PSR, many consumer credit firms rely on third-party payment services for collections, refunds, and consumer disbursements. Key changes may include:

- **Greater regulatory oversight of third-party payment partners**, with knock-on effects on operational due diligence and outsourcing governance
- **Heightened expectations for transparency and consumer fairness**, especially where credit repayments are facilitated through newer payment platforms
- **Broader alignment with FCA priorities**, such as financial inclusion and vulnerability protections, which could influence payment-related policies.

3. Fintechs, Challenger Banks, and Embedded Finance Platforms
As financial services become more embedded and platform-driven, these firms will benefit from:

- **Clearer regulatory pathways** and a unified supervisory voice for innovative products that straddle traditional regulatory categories
- **Faster engagement cycles** with a consolidated regulator equipped to respond to market-led developments in areas like variable recurring payments and digital wallets
- Stronger policy integration between payment infrastructure and consumer finance regulations.

Preparing for What's Next

Firms across financial services should treat this merger not as an isolated structural change, but as a signal of future regulatory convergence. Now is the time to:

- Map out regulatory dependencies across payment systems, conduct rules, and infrastructure access
- Engage with trade bodies and industry consultations to shape the evolving regulatory framework
- Revisit risk management and consumer outcome frameworks, ensuring readiness for deeper FCA engagement across previously PSR-specific domains
- Futureproof partnerships and supplier relationships by assessing alignment with incoming supervisory expectations.

How BDO can help

Whether you're a bank, lender, payment firm, or fintech innovator, BDO can support your firm in understanding the regulatory landscape and capitalising on this period of change. Our services include:

- Regulatory strategy and impact assessment
- Governance and compliance framework design
- Consumer Duty implementation and effectiveness reviews
- Supplier and payments partner risk assessments.

BDO's Payments and Fintech team supports firms through regulatory change, business model transformation, and strategic growth. We offer:

- Regulatory health checks and gap analysis
- Consumer Duty readiness reviews
- Licensing and variation of permission support
- Governance and risk framework enhancement.

Please contact us if you would like to discuss how the PSR-FCA merger could impact your business, or how to navigate the upcoming changes.

continued>

If you require support or would like to discuss this topics further, please contact:

luke.patterson@bdo.co.uk or zahra.ellahi@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