IDEAS | PEOPLE | TRUST

Investment and Wealth Management Q3 update 2025

September 2025

BDO

Welcome to your Quarterly Financial Services Sector Update

This edition of the quarterly financial services sector update has a specific focus on the priorities for assurance in 2026 relevant for investment and wealth managers.

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

Sam Ewen
Manager, FS Advisory

+44 (0)7570 728790
sam.ewen@bdo.co.uk

Bruk Woldegabreil
Director

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

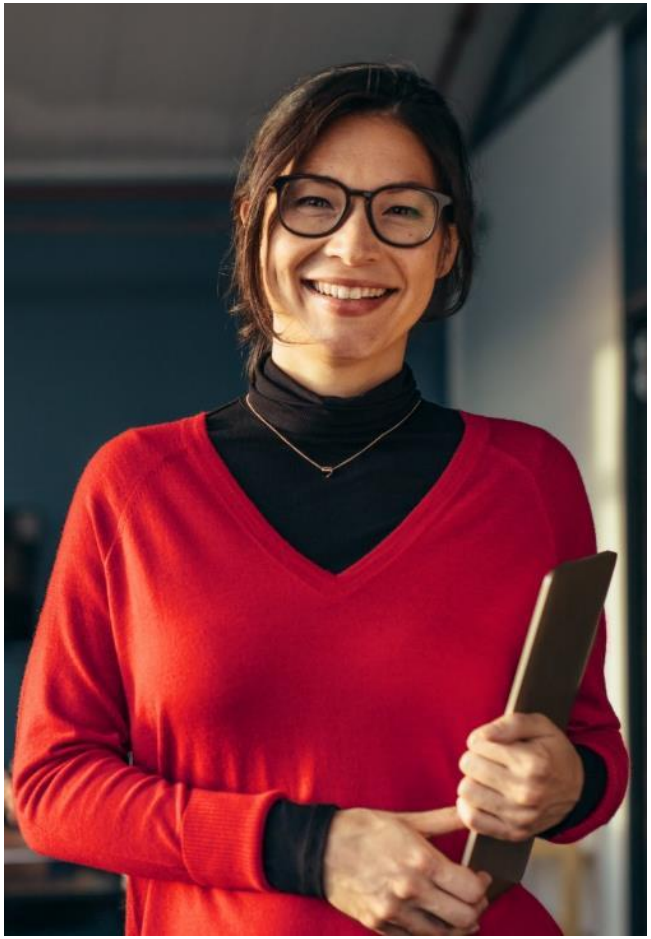
ESG & Accounting Advisory

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

FY26 Assurance Priorities

Appendices

Contents

Other hot topics

Assurance Priorities for FY26

Executive summary

This quarterly update

We hope you had a very enjoyable summer!

As we gather our views on the priorities for assurance in the year ahead, there is a sense of uncertainty, driven by significant global risks. These includes war, cyber threats, national and international debt levels, political stability and fiscal policy changes, all creating potential for further volatility.

Inevitably, resilience is therefore of high importance, but this, along with many of the topics that we consider within this update are not entirely new.

Therefore, as you consider your assurance plans, we hope that this provides a helpful insight into some of the key topics and for each topic, some ideas about the priority areas for focus.

You may pick and choose the topics that are most relevant to you, taking into account your strategic priorities as well as previous assurance activity.

While this update focuses primarily on supporting Internal Audit in planning assurance activities for the year ahead, it will also benefit second-line assurance teams, such as Risk and Compliance, particularly as they seek to coordinate these activities alongside Internal Audit under a combined assurance framework.

We hope that you find this update valuable and we would be happy to discuss your audit plans with you.

01
Corporate governance

Alex Traill
Director

alex.traill@bdo.co.uk

Back to contents

Corporate governance
Hot topics

UK Corporate Governance Code 2024

Overview and key dates

Provision 29 of the UK Corporate Governance Code comes into effect for accounting period starting on or after 01 January 2026.

Drivers - Why should this be considered for audit plan?

The principal requirement of this provision is for the board to issue a declaration over the effectiveness of material financial, operational, compliance and reporting controls as at the balance sheet date.

Firms with a 31 December year end will be fulfilling their obligations under this provision for the first time in 2026. Many will have well advanced plans to tackle the challenge that this presents.

Indicative scope areas:

- Scoping of material controls - evaluate the risk-based, proportionate methodology to scope material controls across financial, operational, reporting and compliance pillars of the code.
- Consideration of dependencies and key underlying controls - review of how dependencies and interdependencies (e.g. IT general controls, third-party reliance, entity-level controls) are identified, mapped and reflected in assessing control effectiveness.
- Roadmap for effectiveness assessment - examination of the plan, timelines, responsibilities, governance and escalation for design and operating effectiveness testing, remediation and continuous improvement.
- Assurance framework - review of the proposed, risk-based and proportionate approach to obtaining assurance over material controls.
- Review of proposed annual report disclosures in comparison to activities undertaken and outcomes achieved.
- Readiness for compliance to meet Provision 29, aligned to UK Corporate Governance.
- Code principles, highlighting gaps, risks and required enhancements.
- Assess proposal for BAU Provision 29 activities in future reporting periods, including ownership responsibilities and reassessments of appropriateness of material controls and related assurance activities.

Suggested time required: 5-10 days

Where conflicts arise, Internal Audit teams should consider the requirements under the Standards and Code to maintain independence and safeguard objectivity, specifically Standards 2.3 and 7.1 and Principle 21 of the Code.

02

ESG and sustainable finance

Sasha Molodtsov
Partner

sasha.molodtsov@bdo.co.uk

Gloria Perez-Torres
Associate Director

gloria.pereztorres@bdo.co.uk

Back to contents

ESG and sustainable finance
Hot topics

PRA's enhanced climate change risk management expectations for banks and insurers

Overview and key dates

The PRA first published its expectations for firms in 2019 in SS3/19. Consultation Paper 10/25 released on 30 April 2025 *"Enhancing banks' and insurers' approaches to managing climate-related risks – Update to SS3/19"* sought views on a draft of updated expectations.

The final update to SS3/19 is expected in Q4 2025 and it will be effective on the date of the publication.

From the date of publication, The PRA proposes a six-month grace period for firms to conduct a gap analysis against the new expectations and prepare an action plan to enhance their climate risk management frameworks.

Drivers – Why should this be considered for audit plan?

Firms should conduct an internal review of their status in meeting existing and updated expectations. Where gaps are identified, firms should develop a plan for how they will be addressed (including interim actions).

Internal Audit teams are best placed to support firms by reviewing the gap analysis expected by the PRA.

Post-grace period, the PRA may ask firms to evidence their internal assessments, gap analyses, action plans or other steps taken to meet the updated expectations.

Indicative scope areas

Review the gap analysis conducted by the firm and evaluate whether it covers all the enhanced expectations set out in the updated SS3/19, including:

- Governance arrangements for Board and senior management oversight and monitoring of climate risks.
- Climate Risk Framework design and operational effectiveness.
- Stress testing and scenario analysis including enhancement plans for the ICAAP/ORSA.
- Disclosures and alignment with TCFD recommendations.
- Approach to identifying, assessing, and acting upon any gaps including how consequent uncertainty in their assessments is quantified and considered from a risk appetite and risk management perspective.
- Any plans to report in line with the UK's Sustainability Reporting Standards (SRS) in 2026/2027.
- Review and evaluate the firm's action plan and roadmap to enhance the climate risk framework to assess whether it is realistic, viable and has appropriate governance arrangements.

Suggested time required: 15–20 days

Greenhouse Gas (GHG) emissions and sustainability disclosures

Overview and key dates

2018 Streamlined Energy and Carbon Reporting (SECR) requirements for medium and large sized firms from 01 April 2019.

Taskforce on Climate-related Financial Disclosures (TCFD) reporting from 2020.

Energy Savings Opportunity Scheme (ESOS), phased implementation, phase 3 from 06 August 2024.

Drivers – Why should this be considered for audit plan?

The regime is the UK's primary framework guiding energy and carbon information reporting. It applies to large UK companies, including all quoted companies, large LLPs, and large unquoted companies, requiring them to disclose their energy use, GHG emissions, and related information in their Directors' Reports.

The criteria for being 'large' is defined as meeting at least two of the following:

- Annual turnover of £36 million or more
- Balance sheet total of £18 million or more, or
- 250 employees or more.

continued >

Back to contents

ESG and sustainable finance
Hot topics

These climate-related reporting frameworks require the collation, calculation and reporting of GHG emissions and sustainability related data.

SECR compliance is more than a regulatory requirement; it reflects a company's commitment to corporate responsibility and environmental stewardship. Many firms adhere already to the regime and voluntarily report annually.

Internal audit can support the business to ensure the controls for reporting are robust. Statutory audits only conduct substantive procedures over sustainability reporting due to a heightened risk of misstatement.

Indicative scope areas

- Assess the governance arrangements for GHG reporting controls in terms of collection, processing and reporting, by assessing the completeness, accuracy, timeliness of qualitative and quantitative data, including for quality assurance.
- Review the governance oversight and control environment including the clarity of roles responsibilities and accountability, formalisation of processes, KPI monitoring, control and methodology.
- Assess the assumptions and methodology framework applied within the GHG emissions preparation and finalisation against a relevant framework such as the GHG Protocol and the Partnership for Carbon Accounting Financials ("PCAF") guidance.

Suggested time required: 15-20 days

Taskforce on Climate-related Financial Disclosures (TCFD)

Overview and key dates

TCFD-aligned requirements (for climate-related reporting) are already in force in the UK, for listed companies via the FCA's listing rules and for the largest private companies and limited liability partnerships via the Companies Act 2006.

Trustees of larger occupational pension schemes and authorised master trust and collective money purchase schemes are required to use the TCFD recommendations to consider climate-related matters in their governance processes since October 2021.

In H1 2025, the FCA carried out a review of TCFD reporting among asset owners and managers through desk research and industry engagement. A summary of the findings and their next steps, will be published in H2 2025, including updates on the interplay between TCFD and SDR entity-level disclosures.

The FCA will consult in H2 2025 on proposals to mandate the use of UK SRS for FCA regulated firms.

Drivers - Why should this be considered for audit plan?

Firms should consider FCA feedback on TCFD Implementation which included forward-looking data and metrics like scenario analysis and climate value at risk; data comparability due to variations in methodologies used for scenario analysis; proportionality as some reports were highly technical, and accessibility to product reports which were difficult to find at times.

Continued roll-out of mandatory reporting. Latest cohort of firms subject to mandatory reporting is asset managers with >£5bn AUM, who had to report by 30 June 2024.

Indicative scope areas:

- Assess the design of the controls around the production of the TCFD entity-level and product-level reports.
- Assess the content of the TCFD reports against regulatory expectations and industry good practice.
- Assess the suitability and sufficiency of the Management Information ("MI") reported to relevant governance forums in respect of the sustainability-related objectives, and review how firms are, or plan to monitor progress against these.

Suggested time required: 15-20 days

Back to contents

ESG and sustainable finance
Hot topics

ESG strategy and transition plans

Overview and key dates

For firms subject to TCFD reporting (phased roll out since 2020), the development of at least a climate-related strategy is mandatory.

The Department of Energy Security and Net Zero is consulting on a transition plan proposal for financial institutions to be required to develop a transition plan and disclose as part of their annual reporting.

Drivers - Why should this be considered for audit plan?

Regardless of mandatory sustainability-related requirements, all regulated firms should have at least demonstrated consideration of developing an ESG strategy or plan, which is proportionate to the materiality of sustainability-related risks faced, including regulatory risks.

N.B. where a firm is "not ready" for such an audit because they have not begun their ESG strategy journey. [click here to read how we can support you]

Some financial institutions have already developed transition plans and net zero strategies. However, this will be new for most, hence early engagement is advised.

Indicative scope areas:

- Assess the materiality assessment conducted by Management to identify and determine the potential impact of sustainability-related risks to its business.
- Assess the quality and coherence of ESG/sustainability/corporate social responsibility strategy and framework against regulatory requirements, and industry practice and expectations.
- Carry out a gap analysis against the guidance and recommendations by the Transition Plan Taskforce.

Suggested time required: 15 days

Anti-Greenwashing Rule (AGR)

Overview and key dates

Effective since 31 May 2024 as part of its Sustainability Disclosure Requirements ("SDR") and investment labels regime ("PS23/16").

All authorised firms need to meet the rule, which is intended to complement and be consistent with existing financial promotions rules and expectations.

Drivers - Why should this be considered for audit plan?

The AGR is a key requirement introduced by the FCA.

FCA have communicated expectations via several channels including their SDR landing page. They have indicated that it will be monitoring firms' sustainability-related claims about their own operations, products and services.

Detailed guidance (FG24/3) has been issued.

Firms are expected to have implemented policies, procedures and controls to ensure they meet the rule.

Indicative scope areas

- Assess the completeness of AGR controls to understand how compliance is being ensured.
- Assess the extent to which there are controls in place to ensure sustainability-related claims and references within the TCFD and/or sustainability reports are clear, fair, not misleading, and able to be substantiated.
- The approach to retaining evidence of anti-greenwashing quality assurance and sign-off controls.
- Test a sample of sustainability-related claims made about products and / or services and assess compliance against FG24/3.

Suggested time required: 10-15 days

Back to contents

ESG and sustainable finance
Hot topics

Sustainability Disclosure Requirements (SDR) and Naming and Labelling Regime

Overview and key dates

Phased implementation starting with the AGR effective 31 May 2024.

In-scope sustainable investment product naming and marketing rules applied from 2 December 2024, on-going product reporting December 2025 and entity level disclosures from December 2026.

Stewardship Code 2026, published on 03 June 2025, to take effect from 01 January 2026. It puts more focus on demonstrating outcomes, reduces reporting burden through fewer principles, updates definition of stewardship, and offers targeted guidance for different types of signatories.

Drivers - Why should this be considered for audit plan?

FCA has clarified the interaction timing of TCFD and SDR reporting. Firms can link their TCFD reports within their sustainability reports and can meet TCFD rules within the SDR reports as one report.

A large firm (>50bn AUM) in scope of SDR can align reporting periods to produce a single report by June 2026. Until then, two reports are needed in 2025: a TCFD report by 20 June and an SDR report by 02 December (with TCFD disclosure linked or included). From 2026, firms may issue one aligned report by 30 June each year.

On the Stewardship Code, 2026 will be treated as a transition year and existing signatories submitting a renewal application will remain on the signature list throughout the period. It will be important for asset owners, managers, and services providers to familiarise themselves with the Code and respond accordingly, in due course.

Indicative scope areas

- Assess the design of the controls around the production of the entity-level and product-level reports
- Assess the content of the reports against regulatory expectations and industry good practice.
- Review the firm's approach to considering the interaction between the SDR reports and alignment with any other TCFD and sustainability reports the approach and timeline meets FCA's expectations.
- Assess the suitability and sufficiency of the Management Information ("MI") reported to relevant governance forums in respect of the sustainability-related objectives, and review how firms are, or plan to monitor progress against these.

Suggested time required: 15-20 days

Diversity and Inclusion

Overview and key dates

Existing FCA rules and expectations for healthy cultures, Board diversity and succession planning since 2022.

The FCA's final policy decision for proposals was set in 2022 within the CP21/24 - Diversity and inclusion on company boards and executive committees.

In July 2025, the FCA also clarified their expectations on bullying, harassment and violence to deepen trust in financial services.

Drivers - Why should this be considered for audit plan?

These FCA measures see to improve transparency on the diversity of company boards and their executive management for investors and other market participants.

For listed firms:

- FS Corporate Governance Code updates
- FTSE Leaders and Parker Review expectations
- IA Standards: CIIA 'Auditing D&I' technical guidance

continued >

Back to contents

ESG and sustainable finance
Hot topics

Industry led public charters/ membership bodies:

- Women in Finance Charter
- Race at Work
- Progress Together
- Diversity Project

Assessment of firms Diversity, equity, inclusion and belonging (can also be included within talent, culture and broader ESG remits) arrangements to ensure regulatory compliance, and in line with industry and market expectations.

Indicative scope areas

Governance and responsibility

- Review Terms of Reference for the Board and Board Nomination Committee (NomCo).
- Review statements of responsibility for Board members, Chair of the Nomination Committee (NomCo), Chief Executive Officer and the Chief People Officer.
- Review governance structure for reporting D&I matters internally across the Bank (i.e. to Senior Management/SMFs).

D&I documentation

- Review D&I strategy, D&I plans/Charter.

Reporting & M.I

- Review the data that is reported internally to Senior Management and the Board in relation to D&I, including the Group Scorecard.
- Review the data that is reported externally (i.e. gender pay gap, ethnicity pay gap).

Employee lifecycle

- Review the processes to attract and recruit new employees.
- Review processes in place to retain, promote and encourage internal mobility for employees.
- Review employee exit process.

Board succession planning

- Review how the Board performs succession planning (i.e. focus on skills, experience and effectiveness of its members).
- Review ExCo succession planning and consideration of D&I.

Non-Financial Misconduct

- Review design and effectiveness of whistleblowing and speak up arrangements.

Suggested time required: 15 days

Back to contents

ESG and sustainable finance
Emerging trends

EU Corporate Sustainability Reporting Directive (CSRD)

Overview and key dates

In February 2025, the European Commission launched its Omnibus I initiative, aimed at reducing the sustainability reporting burden on companies, with proposals for major changes to a series of regulations, including the CSRD, the Corporate Sustainability Due Diligence Directive (CSDDD), as well as the Taxonomy Regulation, and the Carbon Border Adjustment Mechanism (CBAM).

For third country firms (e.g. UK) that have significant operations in the EU, the CSRD will apply on a phased implementation basis, expected between 2026-2028.

Drivers - Why should this be considered for audit plan?

Rules, requirements, and timeline, as well as the need for mandatory assurance over disclosures, will be determined in 2025–2026.

Indicative scope areas

- An assessment of the planned governance arrangements for CSRD reporting controls in terms of collection, processing and reporting, by assessing the completeness, accuracy, timeliness of qualitative and quantitative data, including for quality assurance.
- Assess the methodology by which the firm has conducted or will conduct its “double materiality assessment”.
- Review the governance oversight and control environment including the clarity of roles responsibilities and accountability, formalisation of processes, KPI monitoring, control and methodology.
- Evaluate the assumptions and methodology framework applied as per the CSRD and technical guidance.

Suggested time required: 15 days

Taskforce of Nature-Related Financial Disclosures (TNFD)

Overview and key dates

TNFD was launched in June 2021.

It provides a framework of recommendations for voluntary reporting on nature-related risks and opportunities.

It aims to standardise and improve reporting on the impact of business activities on nature, helping organisations assess and manage nature-related risks and opportunities effectively. It is also an avenue to channel capital flows into positive action.

Drivers - Why should this be considered for audit plan?

Firms that adopt the TNFD recommendations need to implement a strategy for nature and biodiversity and a framework for nature-related financial disclosures to be published on a yearly basis, where this is possible.

Indicative scope areas

- Assess how nature risk considerations are incorporated into the firm’s wider ESG and/or climate risk universe.
- Evaluate the process and methodology for identifying materiality dependencies, risks impacts and opportunities
- Review the quality and coherence of nature and biodiversity strategy and roadmap against TNFD and Climate Financial Risk Forum (CFRF) Guidance, industry practice and expectations.

Suggested time required: 15 days

Back to contents

ESG and sustainable finance
Emerging trends

UK Government consultations

- UK Sustainability Reporting Standards: UK SRS S1 and UK SRS S2
- Transition Plans
- Oversight regime for assurance of sustainability-related financial disclosures
- Forthcoming FCA consultation on its proposals to require the use of UK SRS within its listing rules.

Overview and key dates

The UK Government has set out its ambition to deliver a regulatory framework to support sustainable growth. For this purpose, the Government published three key consultations on 25 June 2025 which will determine future reporting requirements.

The consultations close on 17 September 2025.

The FCA consultation is expected in the next few months.

Drivers - Why should this be considered for audit plan?

UK Sustainability Reporting Standards: UK SRS S1 and UK SRS S2

The UK SRS will be considerably more comprehensive than existing requirements, which are based on the TCFD framework.

This will require financial institutions in scope to provide more detailed, consistent and comparable information on a wider range of sustainability-related risks and opportunities, going beyond climate to include other sustainability factors.

Transition Plans

Depending on the outcome of the transition plan consultation, financial institutions and FTSE 100 companies will need to develop and implement credible transition plans that align with the 1.5°C goal of the Paris Agreement.

Whilst some firms have developed transition plans and net zero strategies, for others this will be new, hence early engagement is advised.

Assurance regime for sustainability-related financial disclosures

The third-party assurance consultation relates to whether a register of sustainability assurance providers should be established. This will impact how firms select their assurance provider.

Indicative scope areas

- The final actions for firms will be determined based on final Government policy.
- In the meantime, firms should engage with the proposals and provide feedback.
- Internal Audit can assess the approach, methodology and content of existing transition plans, when this have been already developed.

03

Culture and behavioural risk

Jennifer Cafferky
Associate Director

jennifer.cafferky@bdo.co.uk

Alison Mackey
Associate Director

alison.mackey@bdo.co.uk

Back to contents

Culture and behaviour
Hot topics

Culture

Drivers - Why should this be considered for audit plan?

- Regulatory focus on culture and conduct – e.g. recent Non-Financial Misconduct policy statement and proposed guidance.
- Business imperative - benefits can include increased engagement and productivity, higher job satisfaction and well-being, supporting the attraction and retention of talent, amongst others.
- Culture can be a risk enabler or a risk mitigator, and having the right culture in place can be a key risk mitigator.

Indicative Scope

Purpose

- Assess whether the Firm's purpose, values, and mission statement are clearly documented. This will include reviewing key documentation, including the Firm's website, strategy, and key people policies (e.g. code of conduct/employee handbook).
- Assess whether the Firm's purpose and values are embedded. For example, is there a clear understanding across the Firm of purpose and values? Are reward and recognition schemes aligned to firm purpose and values? Is there MI in place to support ongoing monitoring of adherence to firm purpose and values?

Review of the key people policies, processes, and practices

- Review the Firm's culture framework (if in place).
- Review the Firm's code of conduct and/or employee handbook.
- Review the Firm's recruitment process to assess whether there is consideration of alignment to firm culture.
- Review the Firm's induction programme to assess whether/how firm culture (including purpose, values, and mission statement) are emphasised.
- Review the Firm's ongoing training programme to assess whether/how culture is promoted via regular ongoing training.
- Review the Firm's remuneration and incentive schemes to assess whether/how these are aligned to firm purpose and values and are conducive in driving positive behaviours. This should include consideration of non-financial (e.g. recognition) as well as financial incentives.
- Review the Firm's wellbeing framework, including whether the Firm has (and makes clear) initiatives to support staff's health and wellbeing (e.g. this may include mental health first-aiders and champions).
- Assess the adequacy and effectiveness of the Firm's channels for receiving employee feedback. For example, regular anonymous surveys, suggestion boxes, feedback forums.
- Review the Firm's leavers process, including the adequacy of exit interviews and surveys, and how this information is monitored and used to drive continuous improvements. For example, do exit surveys request feedback on firm culture?

Review of the Firm's leadership, including "tone from the top" in respect of culture

- Review the Board terms of reference to assess the appropriateness of documented board responsibilities in respect of setting and monitoring firm culture.
- Review a sample of communications from the Firm's leadership (e.g. internal communications) to assess the "tone from the top". For example, are communications frequent enough? Are they clear? Are messages aligned to firm purpose and values? Is there a sense of transparency and openness, particularly in terms of key decisions or strategy?

continued >

Back to contents

Culture and behaviour
Hot topics

Review of the governance and MI framework in place in respect of culture

- Review of the Firm's governance framework to assess clarity of roles and responsibilities in respect of culture. For example, is there clear ownership of cultural objectives at different levels of the organisation? Which committees have responsibilities in respect of culture? Is this clearly documented?
- Assess the adequacy of escalation channels, including Whistleblowing policies and procedures. To include an assessment of whether such channels, and policies, and communications from senior management are conducive to a psychologically safe environment.
- Review a sample of recent culture MI to assess the appropriateness of this. For example, which committee(s) review MI related to culture? Does the Board have sight of culture-related MI? How frequently is such MI produced? Are there sufficient metrics? Are metrics appropriate? Is there sufficient qualitative and quantitative analysis? (e.g. exploring the reasons for attrition and making use of exit interviews and surveys). Is there evidence of root cause analysis? Where risks/issues are identified, how are these addressed? Is this evidenced by the MI.

Suggested time required: 15-35 days

Behavioural risk

Drivers - Why should this be considered for audit plan?

- New IIA Topical Requirement for Organisational Behaviour (consultation period closed in August 2025).
- Regulatory focus on how Firms drive a 'healthy' culture. This includes determining the desired culture and expected behaviours, with measuring, monitoring and reporting being in place for Boards and management.
- Behaviours are the root cause of business success, or failure. Through exploring and assessing drivers of behavioural risk including decision making, leadership, and how errors are managed, Internal Audit can provide evidence-based assurance which prevents risk.

Indicative Scope

Scope and approach are tailored for each firm depending on the assurance objective and unique context of that firm.

Behavioural risk reviews can be used in different ways, as described in the following scope options:

Behavioural risk deep dive

Objective: Identification of patterns of undesirable employee behaviours which impact a firm's ability to achieve its strategic objectives.

Approach: Use of qualitative and quantitative methods to gather a range of data which is analysed and patterns identified. Generally covering a specific business area, or entire firm (for organisations of <250 employees)

Scope: 'Top-down' (firm-wide purpose, values, expected behaviours and tone set by senior leadership). 'Bottom-up' (the employee's day-to-day 'reality', including how the intent from leaders is experienced)

Behavioural risk effectiveness review

Objective: To support the assessment of operating effectiveness, where the Firm has identified processes and controls in relation to the three areas of the topical requirement. This review will assess the 'lived reality' of employees and support an opinion on how specific mechanisms/processes/controls are being used and experienced across the Firm.

Approach: Use of qualitative and quantitative methods to gather a range of data from various business areas, which is analysed and patterns identified.

Scope: Dependent on the process/framework/mechanism requiring assessment.

Suggested time required: 15-35 days

04

Consumer Duty

Tom Story
Senior Manager

thomas.story@bdo.co.uk

Back to contents

Consumer Duty
Hot topics

Embedding the Consumer Duty regulation

Overview and key dates

The Consumer Duty came into force on 31 July 2023 for open products and services and 31 July 2024 for closed products and services.

The FCA is currently seeking feedback on simplifying Consumer Duty requirements and intends to share an update in September 2025.

Drivers - Why should this be considered for audit plan?

One of the FCA's strategic priorities is to help consumers and the Consumer Duty Regulation is the FCA's 'flagship' regulation designed to improve market conduct and consumer outcomes.

Firms should have embraced and embedded a higher standard of consumer protection in its culture and conduct and have systems and controls in place to assess the outcomes customers experience and identify where action is required when these standards are not being met.

Indicative Scope

- Assess the level of engagement at senior committees and the Board in overseeing decision making in line with defined consumer outcomes.
- Assess the embeddedness of the Consumer Duty through comprehensive MI, reporting, root cause analysis, decision making and action execution.
- Assess reporting to Firms' governing body, and Annual Board Report on the outcomes experienced by customers and embedding of the regulation.
- Assess the controls in place to support good consumer outcomes (e.g. in the context of consumer support and engagement).

Suggested time required: 10-20 days

Product governance and fair value

Overview and key dates

All firms are required to have a robust product governance framework for approving new products and reviewing existing products in line with regulatory requirements. Price and Value assessments must also confirm products offer fair value to consumers in the target market.

Drivers - Why should this be considered for audit plan?

The Product and Services outcome in the Consumer Duty regulation requires firms to deliver products and services that meet the needs of consumers.

There has also been significant and continued focus on the fair value of products across the sector, including:

- Failure to pass on changes in interest rates to consumers (Banking)
- Concerns premium finance may not be providing fair value (Insurance)
- Ongoing services fees and charges (Wealth)
- High-cost short-term credit (Consumer Credit)

Indicative Scope

- Assess the design of the product governance and fair value arrangements and execution of those processes.
- Assess descriptions of target markets, distribution channels for completeness and sufficient granularity.
- Assess accuracy of defined roles and responsibilities for product manufacture and distribution (including co-manufacturing relationships)
- The fair value methodology should be clearly documented and consistently applied. It should cover costs, total end-to-end price paid by consumer, value and benefits of the product to the customer. There should be identification of customer cohorts and analysis that fair value is delivered to cohorts, including vulnerable consumers.

Suggested time required: 15-25 days

Back to contents

Consumer Duty
Hot topics

Vulnerable Customers

Overview and key dates

The Consumer Duty regulation was introduced with an objective of raising standards of customer care, including for customers in vulnerable circumstances.

In March 2025, the FCA published the results of its wide-ranging review into vulnerable customer outcomes and the adoption of the FCA's guidance by firms.

Drivers - Why should this be considered for audit plan?

The FCA's fieldwork found examples of positive actions that firms had taken and a renewed focus among firms on delivering good customer outcomes. However, it also found some areas for improvement. These include:

- Consideration of vulnerability in product and service design
- Identification and support of vulnerable customers
- Oversight and reporting of vulnerable customer outcomes.

The FCA wants to see vulnerable customers experience outcomes as good as those for other consumers and to receive consistently fair treatment. In view of the FCA's feedback, firms should ensure that they have appropriate support and controls in place to mitigate the risk of poor vulnerable customer outcomes.

Indicative Scope

Assess the design of product governance processes and, when launching new products or services, whether testing includes consideration of vulnerable customers.

- Assess whether product and fair value assessments are data-led and include specific datapoints for vulnerable customers.
- Test the tailored support offered to vulnerable customers and whether this does support good outcomes for vulnerable customers.
- Assess the appropriateness of training and guidance for frontline staff to identify and offer support to vulnerable customers.
- Test the appropriateness of vulnerable customer MI and whether this provides a clear line of sight into outcomes experienced, with root cause analysis and action taken.

Suggested time required: 15-20 days

05

Financial crime

Karen Monks
Associate Director

karen.monks@bdo.co.uk

Back to contents

Financial crime
Hot topics

Sanctions risk management

Overview and key dates

Sanctions compliance is absolute – firms who are within or undertake activities within the UK's territory, must comply with the EU and UK financial sanctions that are in force. As a result, firms must have robust systems and controls to manage this risk.

A key area of continuing focus for the FCA is on assessing whether firms are maintaining adequate systems and controls to mitigate the risk of breaching sanctions and facilitating sanctions evasion.

Drivers – Why should this be considered for audit plan?

The unprecedented size, scale, and complexity of sanctions imposed by the UK Government and international partners since Russia's invasion of Ukraine, has further increased focus on firms' sanctions systems and controls.

In 2024/25 the FCA carried out 266 assessments of sanctions compliance across a range of sectors. This has involved assessing firms' controls, using a new analytics-based tool, as well as the use of specific intelligence and reporting.

The FCA's annual work programme for 2025/26 has confirmed that the FCA will continue to engage with firms to strengthen sanctions systems and controls as part of its proactive and targeted supervision.

Indicative Scope

Design effectiveness

- Reviewing policies, procedures, and processes for sanctions screening, including the process for reviewing and escalating alerts for consideration.
- Reviewing the processes for ensuring the completeness, accuracy and timeliness of the data supplied by the source sanctions screening systems.
- Assess the effectiveness of the institution's policy for reviewing sanctions alerts; and evaluating the appropriateness of the monitoring of sanctions alert closure.

Suggested time required: 10–12 days

Operational effectiveness

- Assess the quality of investigations conducted into Sanction Screening alerts

Suggested time required: 1 hour per alert investigated

Fraud risk management – ECCTA failure to prevent offence

Overview and key dates

On 01 September 2025, the UK's new corporate "failure to prevent fraud" offence introduced under the Economic Crime and Corporate Transparency Act 2023 ("ECCTA"), came into force.

Written for publication after 01 September.

Under this new offence, large organisations may be held liable if they "fail to prevent" the commission of a specific, wide-ranging fraud offence by those associated with them. The offence applies to UK-based organisations and those based abroad, so long as there are UK touchpoints.

Organisations found liable of this new offence can be subject to an unlimited fine. It will be a defence if an organisation can show that it had in place "reasonable fraud prevention procedures". The UK Home Office has issued government guidance on what constitutes such procedures.

Under ECCTA, "reasonable procedures" cover the following six pillars: governance, policies and procedures, due diligence, risk assessment, communication, and monitoring.

continued >

Back to contents

Financial crime
Hot topics

Drivers - Why should this be considered for audit plan?

The new corporate criminal offence of Failure to Prevent Fraud under ECCTA, which exposes companies to the risk of investigation and prosecution if they benefit (directly or indirectly) from fraud committed by their employees, agents, subsidiaries or providers of services, where the organisation did not have “reasonable fraud prevention procedures” in place to prevent the misconduct.

Indicative Scope

- Assess the engagement of the Firm’s senior management in preventing fraud. This involves examining whether the leadership has clearly articulated a zero-tolerance stance on fraud and whether this message is communicated effectively throughout the Firm.
- Assess the Firm's procedures for conducting due diligence on individuals (staff) during on-boarding and continued throughout the relationship.
- Assess whether the Firm's fraud policies and procedures are suitable for the scale and nature of its operation.
- Evaluate how the Firm identifies and prioritise the risks of fraud it faces. The risk assessment should be thorough, periodic, and documented with clear methodology for evaluating the likelihood and impact of potential fraud risks.
- Assess how the Firm communicates its fraud policies and procedures to staff and relevant external parties.
- Assess the mechanisms the Firm has in place to monitor and review its fraud procedures.
- Evaluate the GAP Analysis and implementation plan and actions tracker they had in place to meet the 1st of September implementation date.

Suggested time required: 15–18 days

AML - transaction monitoring

Overview and key dates

Firms must conduct ongoing monitoring of the business relationship with their customers. Monitoring arrangements should be risk based, driven by the nature, size and complexity of a firm’s business and form part of its financial crime control framework.

Ongoing monitoring of a business relationship includes scrutiny of transactions undertaken throughout the course of the relationship, to ensure that the transactions are consistent with a firm’s knowledge of the customer, its business and risk profile.

Drivers - Why should this be considered for audit plan?

Effective Transaction Monitoring is a key control for all firms subject to FCA regulation and/or supervision.

Deficiencies in firms' approaches to transaction monitoring, are present in the vast majority of FCA supervisory and enforcement actions.

In November 2024, the FCA published PS24/17, confirming the enhancements made to its Financial Crime Guide, including provision made for more guidance, to help firms in adopting and maintaining automated Transaction Monitoring systems.

Further, in July 2024, the Wolfsberg Group, a prominent association of global banks dedicated to enhancing financial crime compliance standards, released a statement on effective monitoring for suspicious activity. The Group's statement is a call to action for firms to enhance their monitoring systems. This means that firms must assess their own risk profiles and tailor their monitoring systems accordingly, rather than adopting a one-size-fits-all approach.

Indicative Scope

Design effectiveness

- Assess the appropriateness of alert rules/scenarios/typologies/thresholds (including how these are tailored according to the inherent risks), expected nature and frequency of activity of the Firm and its customers.

continued >

Back to contents

Financial crime
Hot topics

- Assess and evidence a transaction risk assessment to support the Firm's decision-making process in implementing appropriate thresholds for rules and scenarios.
- Assess the adequacy and appropriateness of the Firm's procedures in providing guidance and expectations on the level of investigation undertaken to discount/escalate alerted activity and to evidence risk-based judgement and rationale for decision-making where appropriate.
- Assess the adequacy and appropriateness of the Firm's transaction monitoring procedure in providing staff operational guidance on how to use and navigate the Firm's transaction monitoring tool.

Suggested time required: 10–12 days

Operational effectiveness

- Assess the quality of investigations conducted into transaction monitoring alerts

Suggested time required: 0.75 hours per alert + 0.25 hours of QA

Fraud risk management – APP fraud

Overview and key dates

The UK's Authorised Push Payment (APP) Fraud Reimbursement Scheme came into force on 07 October 2024. It requires in-scope payment service providers (PSPs) sending payments through either the Faster Payment System (FPS) or the Clearing House Automated Payment System (CHAPS) to reimburse their customers if they are the victim of an APP scam, subject to certain exceptions.

APP fraud happens when a fraudster tricks someone into sending money to the fraudster's account. According to the UK's Payment Systems Regulator (PSR), there are more incidents of fraud than any other crime type in the UK, with APP fraud accounting for 40% of fraud losses in 2022. The UK is the first country in the world to introduce a mandatory reimbursement requirement.

If a customer becomes aware that they are a victim of APP fraud, they must notify their sending PSP without delay, and in any event within 13 months of making their relevant payment.

The sending PSP must reimburse the victim within five business days. The sending PSP can 'stop the clock' if they need to investigate further (including to gather evidence from the receiving PSP), but the sending PSP must arrive at an outcome within 35 business days, regardless of how many times and for how long they 'stop the clock'.

Having reimbursed the customer, the sending PSP is entitled to compensation from the receiving PSP for 50% of the amount paid to the customer.

Drivers – Why should this be considered for audit plan?

The latest figures show £459.7 million was lost to APP scams in 2023. The new rules have consumer protection, ensuring fair treatment and reducing the risk of fraud.

Adhering to the rule is critical to avoid penalties and ensures regulatory standards.

The FCA's 2025/26 Business Plan sets out the FCA's strategy and outcomes focus for the next 5-years, which includes slower growth in APP fraud.

The FCA's annual work programme for 2025/26 has confirmed that the FCA will continue to engage with partners to lead cross-industry projects, to better understand the flow of illegitimate funds across different types of APP fraud and to better prevent them.

Indicative Scope

- **Operational processes - E**xamine the efficiency and effectiveness of processes related to the prevention, detection and response to APP transactions, including customer interaction, investigations and evidence gathering and relevant MI in relation to complaints referred to the FOS.

continued >

Back to contents

Financial crime
Hot topics

- **Risk management.** Full framework review providing a broader, high-level review of the governance structure, policies and training provided to staff.
- **Compliance review.** Assessing adherence to new APP rules and Consumer Duty requirements.

Suggested time required: 15–30 days depending on depth and breadth of review, size of organisation and complexity of detection solutions involved.

Market abuse

Overview and key dates

The objective of this review is to assess and provide assurance over the design and operating effectiveness of the policies and procedures implemented by the Firm to comply with the provisions of MAR which came into force on 03 July 2016.

Drivers – Why should this be considered for audit plan?

The FCA's 2025/26 Business Plan sets out the FCA's strategy and outcomes focus for the next 5-years, which includes protecting market integrity.

The FCA's annual work programme for 2025/26 confirms that they will continue to protect market integrity through assertive action against market abuse; improving detection and investigation capabilities and deterrence through a range of supervisory, civil and criminal sanctions.

Indicative Scope

Review and assess the design effectiveness on governance and oversight arrangements around market abuse, management information 'MI' produced and escalation of matters, as well as minutes of relevant committee meetings.

Assess the adequacy of the Firm's market abuse risk assessment in line with the scale and nature of the Firm's activity, regulatory expectations and industry best practice.

Assess the design effectiveness of the Firm's market abuse monitoring arrangements, including: the systems and processes used for surveillance of the Firm's (and its clients') trading activities; the appropriateness of the system rules and alerts to identify potential market abuse; and second line monitoring and oversight.

Assess the design and operating effectiveness of the personal account dealing policies and procedures currently in place, with a focus on the processes for approval, monitoring, and reporting of employees' personal trades.

Suggested time required: 15-18 days

06
Tax governance

Martin Callaghan
Partner

martin.callaghan@bdo.co.uk

Back to contents

Tax governance
Hot topics

Senior Accounting Officer ('SAO') compliance

Overview and key dates

The Finance Act 2009 requires 'large' UK businesses (those with annual turnover of £200m or more, or balance sheet assets of £2bn or more - with thresholds applied on a group-wide basis) to submit to HMRC appropriate certifications that they have appropriate tax accounting arrangements in place. There are potential financial penalties (both corporate and personal) for failure to comply with the requirements of the SAO regime.

Introduction of the Failure to Prevent Fraud legislation, effective from 01 September 2025.

Drivers - Why should this be considered for audit plan?

Poor tax governance can expose a business to a number of potential issues, including:

- Increased risk of liability under the Failure to Prevent Fraud legislation.
- Reputational risk with tax authorities, regulators and other external stakeholders.
- Financial risk, either as a result of non-compliance (with associated penalties, interest and lost management time dealing with enquiries), or a failure to access appropriate tax credits and allowances.

The specific key drivers for compliance with the SAO regime are:

- Introduction of the "Failure to Prevent Fraud" legislation, which introduced corporate criminal liability for failure to prevent an associated person carrying out a tax fraud which benefits the business – with a defence from prosecution in having "reasonable prevention procedures". There is an alignment between reasonable prevention procedures under FTPF and 'appropriate tax accounting arrangements' under SAO – i.e. robust SAO controls reduces the FPTF risk.
- Compliance is a statutory obligation for large businesses.
- Increased emphasis by HMRC on good governance and risk management, with SAO compliance providing visible assurance to HMRC.
- The risk of financial penalties and adverse reputational impact with HMRC.
- SAO compliance additionally provides internal assurance to the Board and others as to the robust nature of a business' tax operating model.

Indicative Scope

- We issue an online questionnaire focussed on tax governance and SAO compliance specifically to provide us with a snapshot of the control environment and areas of potential focus.
- We carry out a desktop review of appropriate control and procedural documentation.
- Walkthroughs and interviews are conducted with key tax and finance stakeholders and others (e.g. HR function) as appropriate.
- We benchmark the internal SAO process to HMRC guidance and our knowledge of HMRC's approach.
- We identify good practice, design control weaknesses and recommendations for improvements (where relevant) to strengthen and enhance the SAO framework.
- We draw on our extensive experience of conducting SAO reviews to ensure all relevant lessons learned and regulatory expectations have been adequately captured.

Back to contents

Tax governance
Hot topics

Failure to Prevent Tax Fraud - CCO and FTPF

Overview and key dates

Part 3, Criminal Finances Act 2017 ('CCO') means that if an "associated person" of a business criminally facilitates tax evasion, and the business is unable to demonstrate that it had reasonable procedures in place to prevent such facilitation, the business is guilty of a criminal offence.

The legislation took effect in 2017 and applies to all UK businesses and any non-UK business with some UK nexus.

Following similar principles as for the CCO legislation, (corporate criminal liability for failure to prevent criminality by an associated person) s199, Economic Crime and Corporate Transparency Act 2023 ('FTPF') took effect on 1 September 2025. Tax fraud is included in the list of underlying fraud offences that could give rise to liability under the legislation

Drivers - Why should this be considered for audit plan?

The consequences of a prosecution under either offence includes unlimited fines, reputational damage and the likelihood of regulatory sanction.

The specific key drivers for compliance with the legislation are:

- HMRC has now commenced its first CCO prosecution, and we understand that there are further potential prosecutions in the pipeline.
- HMRC have fed into the FTPF Home Office Guidance, and tax fraud is one of the underlying fraud offences which could give rise to a potential FTPF prosecution. As a consequence, controls to manage tax fraud risk are under the spotlight.
- HMRC consider the Financial Services sector generally to be 'high-risk' in relation to the CCO legislation.
- The potential downside of non-compliance is significant, with potential criminal prosecution, unlimited financial penalty and significant adverse reputational and regulatory impact.
- CCO compliance forms a part of HMRC Business Risk Review with a business being rated high-risk for governance if no steps are taken to comply with the legislation.
- CCO compliance is a common element of M&A due diligence and can be raised by financial institutions as part of financing/re-financing decisions.

Indicative Scope

- We review relevant key documentation areas including risk assessments, policies and procedures to build our understanding of the procedures in place and consider the sufficiency of the documented control environment.
- The documentation is evaluated for suitability, considering the sector, size and complexity of the business.
- As a key element of the defence, we review any risk assessment carried out by the business and benchmark the risk assessment against our experience of leading practice and working with similar organisations.
- We conduct interviews with key staff to establish awareness of the legislation as well as the controls and governance arrangements that are in place.
- We specifically consider the adequacy of mandatory training rolled out within the business.

Back to contents

Tax governance
Hot topics

Tax Control Framework and operating effectiveness

Overview and key dates

Introduction of the Failure to Prevent Fraud legislation, effective from 01 September 2025.

Tax governance and risk management are increasingly on the Board and senior management agenda, as well as front of mind for a wide range of external stakeholders including shareholders, potential investors and, of course, tax authorities and the Regulators.

In addition, those large businesses with a Customer Compliance Manager ('CCM) will be subject to periodic Business Risk Review ('BRR+').

Drivers - Why should this be considered for audit plan?

Poor tax governance can expose a business to several potential issues, including:

- Increased risk of liability under the Failure to Prevent Fraud legislation.
- Reputational risk with tax authorities, regulators and other external stakeholders.
- Financial risk due to non-compliance (with associated penalties, interest and lost management time) or a failure to access appropriate credits and allowances.

Specific drivers for focussing on this are:

- Introduction of the Failure to Prevent Fraud legislation, which introduced corporate criminal liability for failure to prevent an associated person carrying out a tax fraud which benefits the business – with a defence from prosecution in having 'reasonable prevention procedures'. A robust tax control framework aligns with the FTPF defence of having reasonable prevention procedures.
- HMRC is focussing its efforts and supervisory resources on the firms most likely to provide the greatest yield – i.e., those they consider to be at highest risk of non-compliance. They are adopting a risk-based approach which moves away from time and resource-heavy enquiries and investigations. For large businesses, this will involve a periodic BRR+ (frequency based on the designated risk rating), which will involve assessing a business across all taxes against 24 low risk indicators. There has been a significant increase in the number of BRR+ taking place, as well as the level of detail and level of resource required to respond to BRR+ requests.
- The environmental, social and governance ('ESG') agenda. Stakeholders in a firm want to know that the firm has a set of strong principles and values that extends to its approach to tax and governance framework.

Indicative Scope

We review several areas including:

- Tax Governance and Strategy.
- Tax Risk Management.
- Tax Performance Effectiveness.
- Control documentation (e.g. Tax Strategy/ Tax Policy/ Tax Process) is evaluated for suitability, considering the sector, size and complexity of the business.
- Walkthroughs and interviews are conducted with key tax and finance stakeholders and others (e.g. HR function) as appropriate.
- In addition, a technical review of a specified area (or type of tax, e.g. corporation tax/ employment duties/ VAT/bank levy) can be incorporated in the scope of work to establish with greater certainty the effectiveness of the designed control environment.

07

Prudential

Aiza Sace
Associate Director

aizamarie.sace@bdo.co.uk

Osita Egbubine
Associate Director

osita.egbubine@bdo.co.uk

Back to contents

Prudential: Investment and Wealth Management
Hot topics

Liquidity Assessments within the ICARA

Overview and key dates

Review of the design and effectiveness of the liquidity risk management framework and the liquidity assessments carried out by the firm to determine its liquid asset threshold requirement.

Drivers – Why should this be considered for audit plan?

Since the introduction of the Investment Firms Prudential Regime ("IFPR"), the FCA have linked the requirement for in-scope firms to maintain adequate financial resources (capital and liquidity), to the threshold condition of appropriate resources. By this, the FCA refers to resources in relation to quantity, quality and availability.

Given recent global events in the financial markets, the FCA has stepped up its monitoring of firms' arrangements for maintaining adequate liquid resources within its ICARA process. The FCA has provided good and poor practice guidelines to support firms' enhancement of their liquidity processes. Whilst the focus of the FCA's supervisory activity has been on wholesale sell-side firms, the same principles and concerns apply to buy-side firms.

Where firms experience breaches of their liquid asset threshold requirements or provide regulatory reports that show assessments that are unusual compared to peers, these firms could be subject to increased regulatory scrutiny leading to a supervisory evaluation and the imposition of individual liquidity guidance by the FCA.

Indicative Scope

- Assess the design and operating effectiveness of the liquidity risk management framework.
- Assess the robustness of the calculations of the liquidity requirements for ongoing operations and to affect an orderly wind-down.
- Assess the effectiveness of liquidity stress testing and contingency funding plans.
- Assess the effectiveness of governance arrangements over the liquidity risk management functions, including the existence of an appropriate risk culture, setting of escalation triggers, key risk indicators, and level of challenge.
- Assess group interdependencies (including outsourced arrangements) in the firm's liquidity arrangements and the effectiveness of monitoring and reporting over these arrangements.
- Assess the adequacy of expertise within the liquidity risk management function and arrangements to enhance competency of the relevant teams involved in the LRMF.

Suggested time required: 25-35 days

Regulatory Reporting (Prudential)

Overview and key dates

Review the design and effectiveness of the firm's prudential regulatory reporting arrangements.

Drivers – Why should this be considered for audit plan?

The FCA expects all MIFIDPRU investment firms to report financial information via the RegData platform accurately and timely. It considers inaccurate or incomplete submissions to be a potential breach of the conduct rules under SMCR and Principle 11.

In March 2025, the FCA confirmed that its prudential planning and approach relies more on regulatory data. Consequently, submissions based on inaccurate and/or poor-quality data creates a negative loop of extra work as it probes firms' responses and may undermine the effectiveness of responses in the event of market events.

Separately, the FCA has confirmed its intention to initiate supervisory work on firms' data items and reporting processes.

continued >

Back to contents

Prudential: Investment and Wealth Management
Hot topics

Indicative Scope

- Assess the effectiveness of regulatory reporting processes including governance arrangements for internal review and validation
- Assess the accuracy and completeness of regulatory returns submitted by the firm in accordance with the reporting guidelines in MIFIDPRU 9 and SUP 16
- Assess the integrity of data sources and the accuracy of reportable data according to the MIFIDPRU methodology for the calculation of financial information.

Suggested time required: 15-22 days

Transaction Reporting (MIFIR and EMIR)

Overview and key dates

Review the design and effectiveness of the firm's transaction reporting arrangements.

Drivers – Why should this be considered for audit plan?

Transaction reports are required to be submitted to the regulators following the execution of a transaction in a reportable instrument. The reports support the regulators in building a view of systemic risk and detecting market abuse. It is therefore vital that firms' transaction reports are accurate, complete and timely.

In 2025, there have been two fines issued for transaction reporting failures. There have also been new Market Watch newsletters issued covering the FCA's expectations for complete and accurate reporting, governance arrangements and control frameworks, and dealing with identified issues/back reporting.

Recent regulatory commentary have also highlighted impending supervisory activity to ensure firms are submitting accurate reports.

Indicative Scope

- Review and assess the appropriateness of the governance and oversight arrangements around transaction reporting, including review of management information 'MI' produced and escalation of matters through relevant committee meeting minutes.
- Review relevant committee meeting minutes, as well as respective Terms of Reference's ("ToR") for relevant roles to assess clarity of roles and responsibilities.
- Review the adequacy of the policies and procedures in relation to transaction reporting, including periodic review and updates to ensure suitability, completeness, and alignment with current regulatory expectations.
- Review the monitoring measures performed by second line to assess effectiveness in identifying issues, escalating to the appropriate forums and tracking issues to closure.
- Review the training framework in place for trade and transaction reporting, specifically training material provided to all relevant staff, including completion monitoring and reporting.

Suggested time required: 10-20 days

Risk Management

Overview and key dates

Review of the design and effectiveness of risk management frameworks to mitigate prudential risks.

Drivers – Why should this be considered for audit plan?

Payments and e-money firms have increased the scale, breadth and complexity of their activities. As a result, the FCA's priorities for this sector include ensuring that firms' risk management capabilities are proportionate to the nature and scale of their businesses, and compliant with their obligations under Principle 4 of the FCA's Principles of Business and maintain adequate financial resources.

continued >

Back to contents

Prudential: Investment and Wealth Management
Hot topics

To this end, the FCA conducted a multi-firm review of the sector (results published June 2025) and concluded that none of the firms assessed as part of their sample fully met their expectations in areas such as enterprise risk management and liquidity risk management, as have been outlined in publications such as FG20/1.

The FCA identified several areas for improvement across enterprise risk management, liquidity risk management and group risk analysis, and expected that Firm's would take away these actions and ensure robustness of their risk management frameworks.

Indicative Scope

- Review risk management governance, the roles and responsibilities of the Board and senior management in effective risk management and the use of the framework in management decision-making.
- Review the adequacy and appropriateness of the risk identification process ensuring that it adequately covers risks from all sources such as current business, as well as from growth plans, new activities etc.
- Review the process to quantify material residual risks following an assessment of risks and controls.
- Assess the firm's understanding of the distinction between capital and liquidity as resources to mitigate residual risk.
- Review the method and rationale for setting the risk appetite.
- Review the use of stress testing to determine the appropriateness of risk appetite limits and thresholds.
- Review the use of stress testing to support the adequacy of financial resources held, and the ability to recover from severe but plausible stress using appropriate management action or recovery action where appropriate.

Suggested time required: 20-25 days

Wind-down planning

Overview and key dates

Review the design of wind-down plans.

Drivers - Why should this be considered for audit plan?

As part of the FCA's multi-firm review of payments and e-money firms published in June 2025, the wind-down plans reviewed in the FCA's sample were all found to be insufficiently effective in their design.

The FCA considers that all firms, including payments and e-money firms, hold adequate resources to cover their ongoing operations, and to wind-down in a solvent and orderly manner without causing disruption to the market, should the need arise. The expectations around wind-down planning are articulated in numerous publications such as the Wind-down Planning Guide (WDPG), the afore-mentioned FG20/1 as well as a thematic review (TR22/1) conducted in 2022.

Indicative Scope

- Review the governance around wind-down planning including the use of the risk management framework to identify scenarios that may result in a wind-down, when in a stress scenario to trigger a wind-down, and how to begin a wind-down process.
- Review the wind-down plan to ensure it includes all applicable areas of the wind-down planning guide.
- Review the appropriate mitigation of risks arising from reliance on the Group for wind-down planning considering key interdependencies.
- Review whether the financial plan assesses the impact of winding-down in a stress scenario and considers all identified risks and resource requirements as well as their impact on financial position, profit and loss, capital and liquidity position.
- Review whether the operational plan, timelines and financial resources are commensurate to wind-down a firm of the business model and profile applicable.

Suggested time required: 15-18 days

08
Digital

Bradley Duffell-Canham
Director

bradley.duffell-canham@bdo.co.uk

Back to contents

Digital
Hot topics

Cyber Security

Overview and key dates

Review of design and effectiveness of cyber security controls against the NIST or CIS frameworks to prevent or respond to a cyber security incident.

Review compliance with cyber standards and/or regulation.

Drivers - Why should this be considered for audit plan?

The financial services sector is highly dependent on technology and digital platforms to deliver products and services to customers, and enable its core functions, such as payment systems, trading platforms, clearing and settlement systems. The interconnectivity of systems means that a cyber incident can create a contagion risk across other processes which could compromise compliance, reporting or disclosure obligations which could impact credibility and trustworthiness in the market.

Attempting to compromise an organisation via a successful breach is now big business, both at state and criminal enterprise levels. The threat is ever evolving as both technology in place at clients, and the means to hack them, are constantly changing.

New mandatory requirements have been set in EU legislation such as the Digital Operational Resilience Act (DORA) which has been in force since 17 January 2025, and the NIS2 Directive, in force since 17 October 2024. Effective cyber resilience controls remain a requirement of the UK Operational Resilience Act (31 March 2025).

Many organisations maintain ongoing technology frameworks which they must align to such as PCI, ISO27001, and Cyber Essentials+.

Indicative Scope

Three-year rolling plan to cover off the design and operating effectiveness of the following 6 domains from NIST (or equivalent CIS for smaller organisations):

- Year 1 – Govern, Identify
- Year 2 – Protect, Detect
- Year 3 – Respond. Recover

Suggested time required: 25-30+ days

Note - operating effectiveness testing is essential therefore the number of audit days for each year should be minimum 20-30+, depending on the scope and size of the firm. To operationalise this, internal audit functions should evaluate work performed to date to determine which of the six domains are remaining for coverage.

- Penetration tests on behalf of third line to test actual sufficiency of cyber controls.
- Cyber regulation compliance (DORA, Cyber Essentials, NIS2, ISO, PCI).
- Cyber incident response and resilience.

Cloud environments

Overview and key dates

The proliferation of cloud technologies and underlying risks around transition, security and availability make this a high priority area for IA coverage.

Drivers - Why should this be considered for audit plan?

Financial services organisations are increasingly leveraging cloud services for their infrastructure and application needs. This transition is driven by benefits such as scalability, cost effectiveness, and accessibility. However, the adoption of cloud services also presents unique risks and challenges, particularly around:

- Data Security and Privacy - The potential for cyber threats and data breaches remains a persistent risk, given the sensitive nature of the data processed in cloud environments.

continued >

Back to contents

Digital
Hot topics

- **Availability** – It is essential to evaluate the technical effectiveness of disaster recovery and business continuity strategies. This includes assessing cloud specific recovery protocols, redundancy measures, and failover capabilities to ensure robust operational resilience.
- **Governance and adoption** – as more organisations adopt cloud technologies risks can arise around the actual transition from on-premises technology to the cloud.

Indicative Scope

Firms will be on different cloud journeys, so should consider risks as outlined below. Assurance providers should consider the stage and pace of development to determine optimum scope and focus of assurance activity.

Those in adoption phase:

- Cloud migration review.
- Review of cloud adoption strategy (data migration, security standards, compatibility, compute resourcing).
- Review of M365 Modern Workplace (as applicable).

Suggested time required: 15-20 days

Those with more mature cloud environments should consider a three-year rolling programme covering the following:

Security review (year 1)

- Assessing the implementation of robust controls to safeguard confidential information stored in the cloud.
- Ensuring encryption standards are maintained both in transit and at rest.

Suggested time required: 15-20 days

Operations review (year 2)

- Evaluating the effectiveness of disaster recovery and business continuity plans to mitigate downtime.
- Ensuring that cloud service providers offer sufficient redundancy and failover capabilities.
- Reviewing incident response procedures to handle data breaches and service disruptions promptly.
- Assessing the effectiveness of access controls and identity management solutions in the cloud environment.

Suggested time required: 15-20 days

Governance review (year 3)

- Verifying that cloud usage complies with industry regulations such as GDPR, HIPAA, and PCI DSS.
- Conducting regular audits to check compliance with FCA, PRA, EBA guidelines, ISO/IEC 27017, and NCSC principles.

Suggested time required: 15-20 days

Innovation review (any time)

- Supporting the organisation's digital transformation initiatives by ensuring cloud environments are conducive to agile development and deployment practices.
- Ensuring that DevOps practices in the cloud are secure and efficient, promoting continuous integration and continuous delivery (CI/CD).

Suggested time required: 15 days

Back to contents

Digital
Hot topics

Outsourcing and third parties

Overview and key dates

Outsourcing remains prevalent in almost all our clients and is a high priority for regulators.

Drivers – Why should this be considered for audit plan?

Regulatory oversight of outsourcing has progressively intensified over the years, with firms required to manage third-party risk in accordance with the General Data Protection Regulation, as well as the FCA and PRA.

The PRA's recent supervisory statement, SS2/21 Outsourcing and Third-Party Risk Management seeks to augment the operational resilience requirements and promote enhanced robustness over the adoption of cloud services and other technologies, as outlined in the Bank of England's response to the Future of Finance report.

Additional regulatory guidance on outsourcing includes DORA, the European Banking Authority (EBA) Guidelines on outsourcing arrangements and aspects of the EBA Guidelines on ICT and security risk management.

Indicative Scope

- Assessing the IT third party supplier strategy and alignment to company policy.
- Assessing IT third-party supplier risk management including a review of the identification and risk evaluation of third-party suppliers.
- Alignment to specific regulatory requirements such as SYSC 8 and 13.9, SS2/21 Outsourcing and Third-Party Risk Management, and EBA guidelines.
- Evaluating IT third-party supplier governance and oversight to assess whether the mechanisms are adequate and effective.
- Assessing supplier performance and compliance by reviewing management's indicators to ensure that they are relevant, reliable and consistent.
- Assessing supplier contractual clauses around right of audit, SOC reports and due diligence.

Suggested time required: 20-25 days

Resilience

Overview and key dates

With the operational resilience transition period ending in March 2025, regulators have expected resilience activities to become a Business as Usual (BAU) activity. DORA (EU only) has also been live since January 2025 and seeks to drive similar outcomes.

The digitised nature of many of our clients means their reliance on outsourced technology is higher than ever.

Drivers – Why should this be considered for audit plan?

The FCA and the PRA have placed operational resilience at the heart of their regulatory framework, recognising that a resilient financial system is critical to the health of the UK's economy. This focus is sharpening as institutions grapple with an array of challenges, from cyber threats to complex supply chain dependencies.

Regulations compel firms to pinpoint their critical business services, those whose disruption could significantly affect customers, the firm, or the stability of the UK's financial market. Firms are encouraged to engage in a series of activities to comprehend the maximum tolerable period of disruption, identify vulnerabilities, and assess the adequacy and effectiveness of contingency plans.

continued >

Back to contents

Digital
Hot topics

The operational resilience regulatory transition period has ended on 31 March 2025 and since then all-important business services are expected to be fully resilient.

More broadly, resilience of wider areas of the organisation which may not be designated an important business service should still have effective solutions to restore operations within an acceptable time. Third party resilience remains a challenge.

Indicative Scope

- Review of compliance with operational resilience regulation, if not done previously.
- If done previously, review of any remaining work conducted since (notably scenario testing) and confirmation of resilience status as of the 31 March 2025 deadline.
- Business continuity management and disaster recovery review.
- Third party resilience review.
- Cyber incident response.
- DORA reviews (see cyber risk above for more detail).

Suggested time required: 20-25 days

Artificial Intelligence

Overview and key dates

Artificial intelligence (AI) remains a buzz phrase, with increasing adoption over the last few years and represents key risks to key areas such as calculations and outputs where AI based algorithms are used. It can also mean a loss of control as staff are increasingly using internet based generative AI software for processing company data assets.

Drivers - Why should this be considered for audit plan?

The increasing uptake in artificial intelligence in financial services heightens the potential to cause significant issues. Fundamentally, a lack of control around AI can result in:

- Untested algorithms being used to generate what may be unsafe outcomes.
- Personal data or key IP being placed in non-secure environments (predominantly the Internet).
- Uncontrolled changes made to AI models undermining established baselines.
- Use of inappropriate or incomplete inputs to a data model.
- A lack of clarity and transparency around where AI models are used for decision-making.

ISO/IEC 42001:2023(E) provides a base level of expected controls and risks to be managed when using AI. Additionally, the provisional version of the EU AI Act, which came into force in August 2024, will also be useful as initial guidance for expected legislative requirements that organisations need to comply with.

Indicative Scope

- Review of governance around AI and any underlying strategy.
- Verify the accuracy and reliability of data and algorithms being used, including the consistency of outputs and decisions.
- Assess the culture and communication around AI and provide feedback and suggestions for enhancing trust, engagement and collaboration.

Suggested time required: 15-25 days

Back to contents

Digital
Hot topics

IT change programmes

Overview and key dates

With technology roll-outs and enhancements underpinning many organisation's business strategies, digital transformation is a key risk area.

Drivers - Why should this be considered for audit plan?

With IT change programmes, technology is the enabler for new ways of working that can open new markets, enable the deployment of new products more quickly/ efficiently, improve back-office efficiency and create data driven organisations (to mention a few). However, with this level of change, the potential to introduce excessive cost, failed processes and adverse customer experience (with associated regulatory intervention) is extremely high and borne out by the large number of organisations experiencing these issues.

Internal Audit can provide a high level of specialised channel to ensure that the risks around project components are effectively managed and that governance stakeholders are provided with the right information for making 'go/no-go' decisions.

Indicative Scope

Review programme governance, delivery frameworks and planning, to include:

- Functional requirements gathering and scope definition.
- Agile change management and communication.
- Data Strategy, migration, and re-platforming.
- Testing and validation.
- Benefits definition, tracking and realisation.

Suggested time required: 20-25 days

Data governance

Overview and key dates

With data at the heart of accurate management reporting, internal outcomes and customer outcomes, the management of data quality and the ability to make effective use of that data is a high strategic priority for many of our clients.

Drivers - Why should this be considered for audit plan?

All organisations rely on data to run their business and make strategic decisions to drive the organisation forward.

Data governance aims to generate value from data as an asset by minimising the risk of poor-quality data that is subsequently used to make ineffective decisions; which can prove costly. Furthermore, errors in transactional data can undermine customer outcomes and impact the organisation through incorrect calculation of key values such as pricing, interest and claims.

- Review of data governance processes, in particular:
  - Policies and procedures
  - Roles and responsibilities
  - Data discovery, evaluation and classification
  - Data mapping
  - Data quality controls
  - Master data management.
- Specific data migration reviews.
- Evaluation of the accuracy of outputs from key calculation engines, including use of data analytics and data visualisation.
- Data retention and deletion.
- Holistic approach to data governance for managing broader tenets of data such as availability and confidentiality.

Suggested time required: 20-25 days

Back to contents

Digital
Hot topics

Payments Review (SWIFT/Faster Payments)

Overview and key dates

Review of organisation's stated payments technology control to ensure that attestation returns to providers are accurate or that requirements around implementation of payments technology have been met.

Review of the organisation's compliance with the SWIFT Customer Security Controls Framework (CSCF), focusing on attested controls, supporting evidence, and any gaps requiring remediation.

Drivers - Why should this be considered for audit plan?

Key payments providers such as Faster Payments and SWIFT require attestations or independent assurance over the implementation of required technology security and availability safeguards for customers (i.e. banks, insurers) to be gain ongoing access to the payments mechanism

Increasing scrutiny from regulators and card schemes on payment infrastructure security

High-value nature of such transactions and associated reputational risk.

Indicative Scope

- SWIFT attestation reviews.

Suggested time required: 15-20 days

- PSD2 implementation and compliance reviews.

Suggested time required: 20-25 days

- Faster Payments implementation and compliance reviews.

Suggested time required: 20-25 days

IT governance

Overview and key dates

Review of approach to managing key facets of IT to meet organisation objectives.

Drivers - Why should this be considered for audit plan?

Failure to manage the IT function may result in failure of key IT initiatives and the inability to evaluate and mitigate technology risk and optimise use of resources and IT assets.

Indicative Scope

Governance review to cover:

- Governance, roles and responsibilities
- IT strategy
- IT risk management
- IT cost management
- Resource management
- Benefits realisation.

Suggested time required: 15-25 days

Back to contents

Digital
Hot topics

IT general controls

Overview and key dates

Review of mitigation of risk of unauthorised access and change to key applications, operating systems and databases.

Incoming changes to FRC focus on non-financial internal control raises the profile of this for area.

Drivers - Why should this be considered for audit plan?

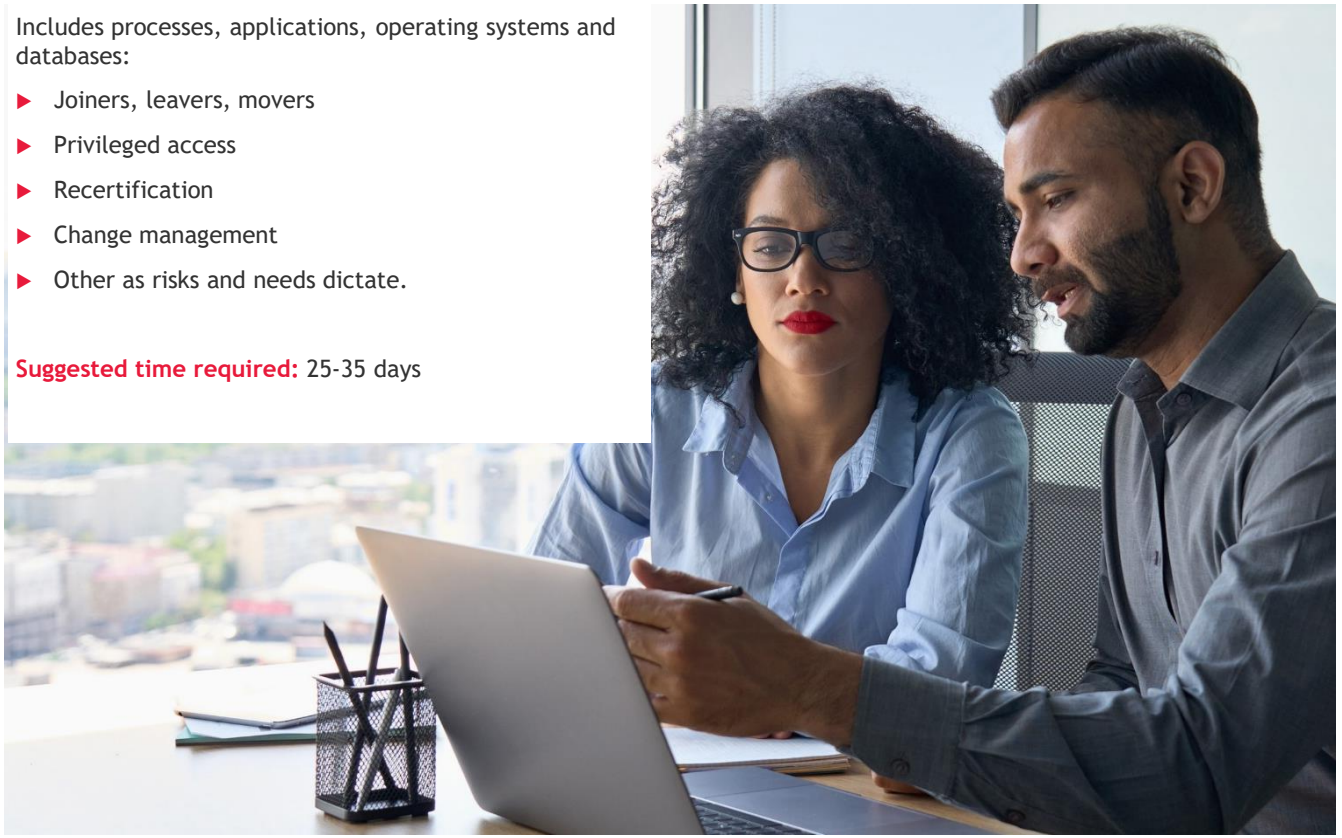
Despite the FRC stating that it will not take forward over half of its original proposals for corporate governance, the revised Governance Code published in January 2024, will place increased focus on internal controls extending beyond finance and including operational and non-financial areas.

Whilst external audit may look at applications material to the financial statements, there may be other applications with underlying operating systems and databases upon which important business services are dependant. Ensuring that access and change is carefully managed is fundamental to the ongoing confidentiality, integrity and availability of the underlying data and transactions within those systems.

Includes processes, applications, operating systems and databases:

- Joiners, leavers, movers
- Privileged access
- Recertification
- Change management
- Other as risks and needs dictate.

Suggested time required: 25-35 days



Other topics of interest

Back to contents

UK National Risk Assessment of Money Laundering and Terrorist Financing 2025 published

The UK's latest National Risk Assessment of Money Laundering Terrorist Financing was published in July. This is the fourth comprehensive National Risk Assessment for the UK, building on previous iterations in 2015, 2017, and 2020 and is a central part of the UK's 'risk-based approach' to countering Money Laundering and Terrorist Financing.

Vladimir Ivanov
Associate Director, FS Advisory

vladimir.ivanov@bdo.co.uk

In July 2025, HM Treasury and the Home Office jointly published the latest National Risk Assessment of Money Laundering Terrorist Financing ("NRA"), as required under the Money Laundering Regulations.

The NRA includes input and expertise from across the public and private sectors including supervisors and law enforcement, whose work is critical in protecting the integrity of the UK's financial system and economy. The NRA is a vital tool in the ongoing work to understand and disrupt the evolving threat posed by criminals and terrorists who try to move their illicit money through the UK financial system, and will be used to directly inform UK policy, regulatory, and operational priorities and responses. For the regulated financial services sector, the NRA provides essential insight into how products/services may be exploited for illicit purposes, and guidance on how these threats can be identified and mitigated.

Key highlights of the NRA

The UK continues to be exposed to a high level of Money Laundering risk

Following Russia's invasion of Ukraine, money laundering, kleptocracy, and sanctions evasion have become increasingly interconnected. Sanctioned individuals and entities are using established money laundering networks, complicit professionals, and complex structures—once mainly used for moving large volumes of criminal funds—to disguise the origins and ownership of their assets.

- Since 2020, the UK's Money Laundering risk profile has shifted significantly due to advances in financial technology:
  - **Electronic Money Institutions & Payment Service Providers ("EMIs" & "PSPs")** – The UK's status as a leading fintech hub has seen EMIs and PSPs become deeply integrated into the financial system. While most activity is legitimate, their widespread use gives criminals more opportunities to disguise illicit activity, increasing overall risk.
  - **Cryptoassets** – Popularity has surged, with growing use in Money Laundering cases, often involving overseas cryptoasset service providers. This trend is linked to rising fraud and ransomware attacks demanding cryptocurrency payments.
  - **Artificial Intelligence ("AI")** – AI offers potential to enhance detection and prevention of Money Laundering, but also creates new risks. Criminals could exploit AI to circumvent controls, commit predicate crimes such as fraud more efficiently, and move illicit funds quickly across larger networks.

continued >

Back to contents

UK National Risk Assessment of Money Laundering and Terrorist Financing 2025 published

- Several long-standing Money Laundering risks remain significant in the UK:
  - **Cash-based laundering** – Despite a decrease in the use of cash, cash-based laundering is still at high levels, involving smuggling, cash-intensive businesses, money mules, and misuse of legitimate channels (e.g., Post Offices) to place illicit cash into the banking system. Criminals often combine cash methods with other laundering techniques.
  - **Financial & professional services exploitation** – Organised criminals continue to use these sectors to integrate illicit funds and benefit from their perceived legitimacy.
  - **UK companies misuse** – High risk persists from both domestic organised crime groups using front companies and cash-intensive businesses, and international high-end criminals exploiting UK corporate structures in complex schemes to launder large sums.
- The threat to the UK from terrorism has remained "substantial" since February 2022, meaning "an attack is likely". Terrorist financing - which involves the use, possession or raising of funds or assets, for the purposes of terrorism, or for the benefit of a proscribed organisation – remains a persistent threat
- Retail banking, EMIs & PSPs, and Money Service Businesses ("MSBs") pose the highest Terorrist Financing threat.

What does this mean for firms?

Financial services firms in the UK should treat the NRA as a foundational input to their own risk assessment framework—not as a standalone document to be filed away. Namely, firms should use the NRA to inform their own Business Wide Financial Crime Risk Assessments ("BWRA"). This does not mean simply referencing the NRA as a source within a firm's BWRA, but rather using the NRA to:

- Cross-check inherent risk categories against NRA findings
- Adding new risk categories where the NRA highlights certain threats or risk indicators that a firm's current framework has not accounted for
- Re-calibrating risk scoring—if the NRA has increased risk ratings for certain geographies, customer types, or sectors, firms should update their inherent risk scores and/or weightings appropriately.

Firms should also use the NRA to inform which areas of their control frameworks require the most attention from an oversight and monitoring perspective. Where the NRA has highlighted either new areas of inherent risk or existing areas subject to increased risk, firms should ensure their Compliance Monitoring and Internal Audit efforts focus on these areas to confirm that mitigating controls are designed and operating effectively.

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

vladimir.ivanov@bdo.co.uk

Back to contents

The UK Data (Use and Access) Act 2025 – Considerations for Financial Services

The new UK Data (Use and Access) Act 2025 came into force on 19th June 2025 and aims to reform some parts of how the UK regulates the processing of personal and non-personal data.

Given the sector's reliance on data for delivering client services, developing new products or services, or to meet compliance obligations, this article highlights the updates that will be most relevant to financial services organisations.

Louise Sadler
Senior Manager, Privacy & Data Protection

louise.sadler@bdo.co.uk

UK GDPR

The UK Data (Use and Access) Act 2025, (hereafter referred to as 'DUAA') does not constitute a considerable overhaul of the UK GDPR but instead has introduced several changes to enhance key areas, with the intention of reducing the burden of the UK GDPR and promoting innovation.

Some of the key changes that Financial Services organisations should be aware of are as follows:

- **Introduction of Recognised Legitimate Interests** – the Act sets out a list of 'recognised legitimate interests', allowing certain security-related activities such as fraud prevention, public safety, and national security to be considered as 'recognised legitimate interests' without the requirement to complete a Legitimate Interests Assessment (LIA).

- **International Data Transfers** - The Act places an emphasis on allowing international data transfers to countries where the protection standard is "not materially lower" than that in the UK. This change is intended to enhance flexibility for businesses engaging in global data transfers.

- **Subject access requests** – Certain financial services organisations receive a high number of subject access requests, which can be both costly and time-consuming to manage.

  The DUAA clarifies that organisations are required to conduct "reasonable and proportionate" searches, which means that whilst organisations are required to make genuine efforts to locate and provide the requested personal data, they are not obligated to conduct exhaustive searches that would impose an excessive burden. This clarification aligns with guidance issued by the Information Commissioner's Office (ICO).

- **Automated decision-making** – The DUAA relaxes automated decision-making rules, meaning that organisations can now use automated decision making for low-risk data processing activities, but only if the principles of transparency and accountability are upheld. Organisations using automated decision making for high-risk data processing activities will still need to apply additional safeguards, in line with data protection requirements. Under the previous framework, individuals had the right not to be subject to decisions based on solely automated processing, including profiling

continued >

Back to contents

The UK Data (Use and Access) Act 2025 – Considerations for Financial Services

Privacy and Electronic Communications Regulations (PECR)

The Act enhances PECR enforcement powers, bringing penalties in line with UK GDPR. It permits fines of up to 4% of global turnover or £17.5 million, whichever is greater, significantly raising potential penalties for electronic communication non-compliance. Financial services organisations are therefore advised to ensure compliance with PECR, particularly regarding cookie usage and direct marketing.

Complaints

The Act requires firms to implement complaints processes which includes acknowledging complaints within 30 days and responding to complaints 'without undue delay.' Financial services organisations should therefore review and update existing internal complaints procedures to reflect these timeframes.

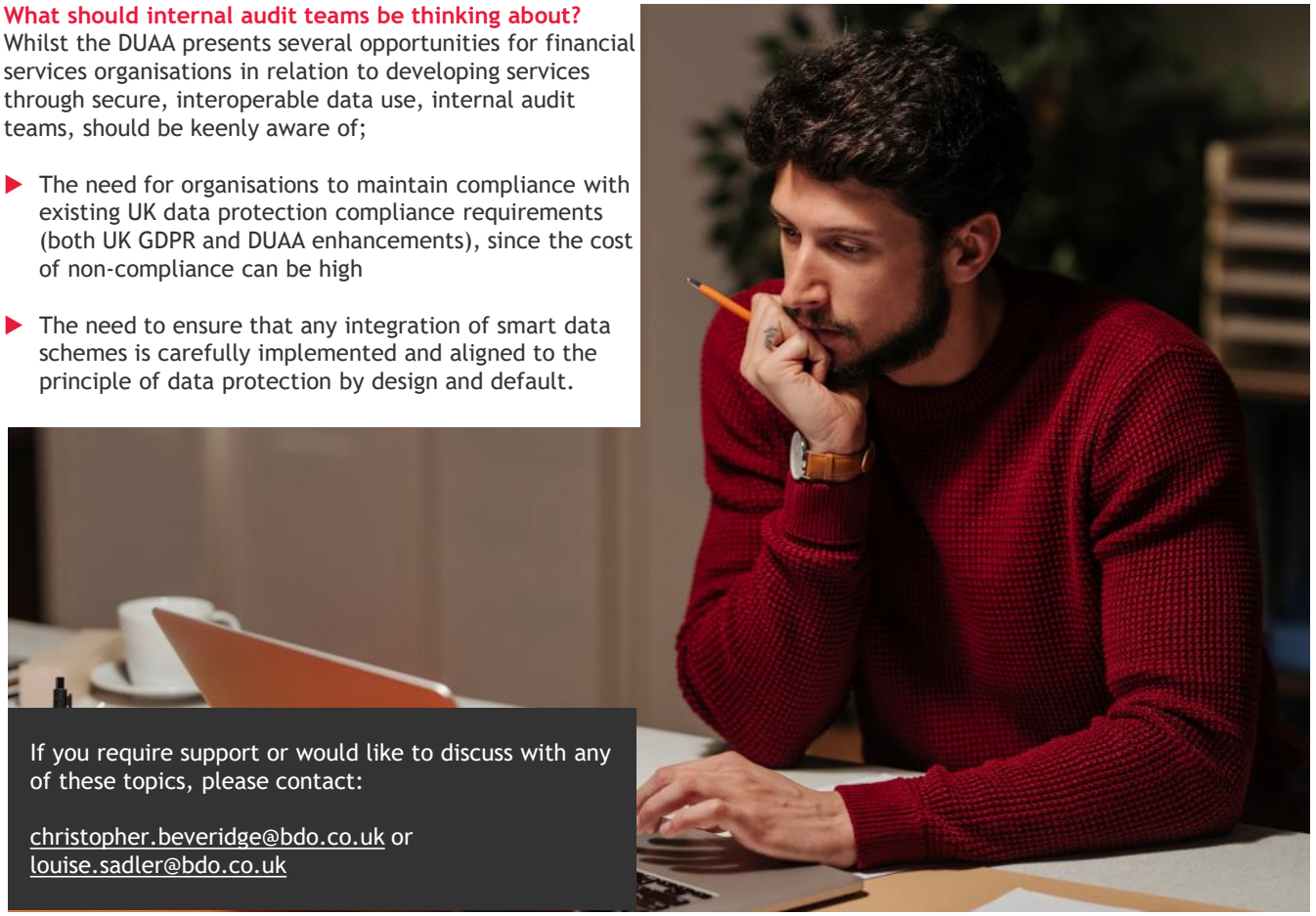
Smart Data Schemes

One of the most significant pillars of DUAA is the new "smart data" scheme which establishes the legal framework. Building on the success of Open Banking the intention is to extend this to other sectors, unlocking access to data but also allowing businesses to securely share customer and business data with authorised third parties, which aims to boost public services and support the UK economy.

What should internal audit teams be thinking about?

Whilst the DUAA presents several opportunities for financial services organisations in relation to developing services through secure, interoperable data use, internal audit teams, should be keenly aware of;

- The need for organisations to maintain compliance with existing UK data protection compliance requirements (both UK GDPR and DUAA enhancements), since the cost of non-compliance can be high
- The need to ensure that any integration of smart data schemes is carefully implemented and aligned to the principle of data protection by design and default.



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

christopher.beveridge@bdo.co.uk or
louise.sadler@bdo.co.uk

Back to contents

Upcoming amendments to FRS 102

Following on from the proposals published in Financial Reporting Exposure Draft 82 ('FRED 82'), the Financial Reporting Council ('FRC') issued amendments to FRS 102 The Financial Reporting Standard applicable in the UK and Republic of Ireland ('FRS 102'). These amendments incorporate, with appropriate simplifications, the five-step model from IFRS 15 Revenue from Contracts with Customers ('IFRS 15') for recognising revenue and the on-balance sheet model from IFRS 16 Leases ('IFRS 16') for the lease accounting that is likely to affect financial statements of most entities having operating leases. The FRED 82 amendments to FRS 102 also include various other incremental improvements and clarifications regarding conceptual framework change and fair value measurement amongst others.

What new elements are introduced in revenue recognition?

This amendment to FRS 102 is reshaping how and when businesses recognise revenue and therefore creating an effect on the profits that entities report in their financial statements. This new accounting requirement for revenue recognition under Section 23 Revenue from Contracts with Customers of FRS 102 ('Section 23') has taken its basis from IFRS 15's five-step model for revenue recognition with appropriate simplifications. This brings transparency and consistency, ensuring that the entity recognises revenue to depict the transfer of promised goods or services to the customer in an amount that reflects the entitled consideration.

Primarily, the five-step model approach to recognise revenue contains the following five steps:

1) Identify the contract with a customer
2) Identify the performance obligations in the contract
3) Determine the transaction price
3) Allocate the transaction price to the performance obligations
4) Recognise revenue when or as the entity satisfies a performance obligation.

Furthermore, the new revenue recognition requirements add more complexities in various areas such that customers options for additional goods or services at a discount, material rights like sales incentives and renewal options, costs to fulfil a contract, licensing and repurchase agreements.

The amendments to FRS 102 bring key simplifications from IFRS 15 and provide transition reliefs. These include:

- Accounting policy choice in respect of the capitalisation of costs to obtain a contract
- Transitional relief to provide an option to either restate comparatives or not to restate comparatives and any cumulative effect of initially applying the amendments is recorded as an adjustment to retained earnings as at the date of initial application.

continued >

Mark Spencer
Partner, Financial Services Advisory

mark.spencer@bdo.co.uk

Vijay Kumar Sharma
Manager, Accounting and Corporate Reporting Advisory

vijaykumar.sharma@bdo.co.uk

Back to contents

Upcoming amendments to FRS 102

What changes are part of the lease accounting amendments?

This amendment to FRS 102 fundamentally alters financial statements and KPIs by bringing previously off-balance sheet lease agreements directly onto the balance sheet using the IFRS 16 on-balance sheet lease accounting model that becomes the basis of the new accounting requirements for leases under Section 20 Leases of FRS 102 ('Section 20').

For lessees, this amendment to FRS 102 will eliminate the distinction between finance leases and operating leases and require recognition of a lease liability and corresponding right of use ('RoU') asset on the balance sheet. The RoU asset will be depreciated until the end of its useful life subject to other conditions or until the end of the lease term and a lease liability will reflect the entity's obligation to make lease payments over the duration of the lease.

As a result of this amendment, most lessees with operating leases will be affected except for those leases that are considered to be short-term, 12 months or less in duration, or relate to low-value items. Therefore, the current operating lease expense, typically rent, will be replaced by depreciation of the RoU asset along with a finance cost for the unwinding of the lease liability.

Furthermore, as this amendment brings complexity in order to identify the embedded leases within a variety of infrastructure contracts, such as fibre-optic cables, dedicated server racks and data centres, even when the contract is not explicitly labelled as a lease agreement.

The FRS 102 amendments bring key simplifications from IFRS 16 and provides transition reliefs as follows:

- Allowing the use of an obtainable borrowing rate
- Accounting policy choices to measure seller-lessee ROU asset for sale and leaseback transactions while IFRS 16 does not
- Transition reliefs including a modified retrospective approach that has no restatement of comparatives but the difference between the asset and the liability are recorded as an adjustment to retained earnings as at the date of initial application and an ability to use balances previously determined for group reporting purposes under IFRS 16.

Other FRS 102 amendments

Other incremental improvements and clarifications to FRS 102 include:

- Greater clarity for small entities in the UK applying Section 1A Small Entities regarding which disclosures need to be provided in order to give a true and fair view
- A revised Section 2 Concepts and Pervasive Principles that is updated to reflect the International Accounting Standards Board's Conceptual Framework for Financial Reporting that was issued in 2018
- A new Section 2A Fair Value Measurement that replaces the Appendix Fair Value Measurement to Section 2 and reflects the principles of IFRS 13 Fair Value Measurement ('IFRS 13')
- As a step towards phasing out the IAS 39 Financial Instruments: Recognition and Measurement option for financial instruments, new adoptions to apply IAS 39 recognition and measurement under paragraphs FRS 102 are being prohibited unless required to align with group accounting policies. Existing users of the IAS 39 option are not affected and can continue applying it
- New disclosure requirements about supplier finance arrangements within Section 7 Statement of cash flows.

What should you do next?

The amendments to FRS 102 will be effective for accounting periods beginning on or after 1 January 2026 with early adoption permitted provided that all amendments are applied at the same time.

continued >

Back to contents

Upcoming amendments to FRS 102

We would recommend that you start planning now for the upcoming changes, beginning with an impact assessment as to understand the effects on your financial statements before 1 January 2026 and identify where you should update systems and processes (which includes charts of accounts) and update accounting policies as well as prepare for increased disclosures in your financial statements.

What effect do the FRS 102 amendments have on Investment and Wealth Management sector?

Based on the five-step model of IFRS 15, the FRS 102 amendments introduce a more prescriptive approach to revenue recognition under Section 23, which is expected to impact the asset management sector significantly.

In the context of revenue recognition for asset management arrangements, this amendment brings complexities such as identifying the customer as funds or the investors, unbundling multiple service obligations that are contained within a single contract, the treatment of upfront fees, the pricing mechanisms that include variability in amounts and capitalisation of costs to fulfil a contract. This change could also affect financial reporting and disclosures, KPIs, compensation plans, loan covenants based on KPIs and ability to distribute profits.

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

mark.spencer@bdo.co.uk or
vijaykumar.sharma@bdo.co.uk

Back to contents

IIA Topical Requirement: auditing organisational behaviour

In July 2025, The Institute of Internal Auditors (IIA) issued the draft Organisational Behaviour Topical Requirement which sees a re-framing of how 'culture' can be audited, with formal recognition that how people behave is a central element of risk in all organisations. The focus will be on assessing behaviours which can either adversely impact a Firm's strategic objectives or drive positive outcomes. The final Topical Requirement, due in September, will establish the minimum mandatory requirements for internal auditors when organisational behaviour is included in the scope of an assurance engagement.

Alison Mackey
Associate Director, Financial Services Advisory

alison.mackey.co.uk

Behaviours as a core element of risk management

The concept of 'auditing culture' has been a considerable challenge for a number of years for IA functions in terms of how to do this in a meaningful way. The Topical Requirement provides Internal Audit teams with an approach to auditing organisational behaviour, specifically, through governance, risk management and controls. This should be viewed as a 'minimum baseline' which can be adopted by all IA functions as part of their risk-based audit approach.

As with all Topical Requirements, they must be applied in conformance with the Global IA Standards and are mandatory for assurance services (recommended for advisory services). Conformance will be assessed through quality assessments.

Summary of Topical Requirement

The IIA define organisational behaviour as:

"The observable actions, decisions, and interpersonal dynamics of individuals and groups within an organisation. This behaviour influences performance and the achievement of strategic objectives."

The evaluation of organisational behaviour is focused on three areas, underpinned by specific aspects which Internal Auditors must assess. In summary:

1) Governance

- Board and senior management structure, roles and responsibilities
- Accountability for behavioural expectations is maintained by the Board and senior management
- Governance processes are in place to monitor and measure the extent to which patterns of behaviour align with the Firm's strategic objectives
- Behavioural risk policies and procedures are established, reviewed and communicated.

2) Risk Management

- The Firm's behavioural risk management process is appropriately defined
- Monitoring of organisational behaviour is in place
- Any gaps between expected and actual behaviours are assessed and shared with management
- These gaps are resolved with the appropriate inputs and tracking.

continued >

Back to contents

IIA Topical Requirement: auditing organisational behaviour

3) Controls

- Use of Behavioural Risk reviews to identify and mitigate patterns of behaviour which present a strategic risk
- Expected behaviours are clearly and consistently communicated with a feedback mechanism in place
- Reporting processes in place to surface organisational behaviour which is misaligned with the Firm's expectations and strategic objectives
- Incentive programmes are established, with consequences for 'improper' behaviours
- Behavioural issues are identified and addressed through embedded processes
- Periodic training for employees to ensure that there is adherence to strategic objectives
- Alignment between behavioural expectations and the Firm's talent/recruitment processes.

The IIA has published a User Guide with illustrative examples of what Internal Auditors may wish to assess as part of an Organisational Behaviour audit. With all Topical Requirements, auditors should apply professional judgement as to how it is applied. This would apply to the inclusion (or exclusion) from the annual plan, and also which aspects would form part of individual audit engagements.

Challenges for Firms

The structure and specificity provided by the Topical Requirement enables Internal Audit teams to make an evidence-based assessment of organisational behaviours.

However, this is working on the assumption that Firms are aware of, have understood and thus established, behaviours as part of their purpose, values and strategy and also their risk management framework, governance and processes.

Many Firms, particularly those which are smaller in size and/or have a less mature risk management approach, may not be in this position. As such, dedicated metrics and reporting of organisational behaviours may not have been developed.

In terms of behaviours and culture, we know that:

- The importance of a 'healthy' culture is recognised by Firms (largely driven by Consumer Duty), but many Firms have not necessarily defined the expected behaviours of its employees
- Culture is largely assessed through employee surveys and certain people data (i.e. attrition rates and exit interviews), with Boards and management receiving metrics and results on a periodic basis. In some Firms, this reporting is very limited
- Some Internal Auditors have been developing an approach to auditing risk culture specifically or developing a suite of cultural indicators for use in each audit engagement.

What initial actions can Internal Audit teams take?

- Review your Firm's purpose, values and strategy and establish how culture and behaviours are incorporated, measured, monitored and reported to the Board and senior management
- Review the current approach to auditing behaviours and culture: assess the extent to which the current approach can be adjusted to align with the requirements (i.e. through a gap analysis)
- Discuss the requirements with 1LOD and 2LOD colleagues: ensure there is transparency around what Internal Audit will be covering as part of future audits
- Establish the 'current state' with your Firm: assess how mature the is Firm in its consideration of 'misaligned' organisational behaviour as a risk. This could be from the 'top-down' in terms of the extent to which expected behaviours have been articulated and established by senior management and through the Firm's governance processes and structures. It should also be understood how behavioural risk is considered as part of the risk management framework and processes

continued >

Back to contents

IIA Topical Requirement: auditing organisational behaviour

- Incorporate organisational behaviour into your Audit Universe, Risk Assessment and Annual Planning process: this will enable you to exercise professional judgement and drive a robust conversation with your Audit Committee.

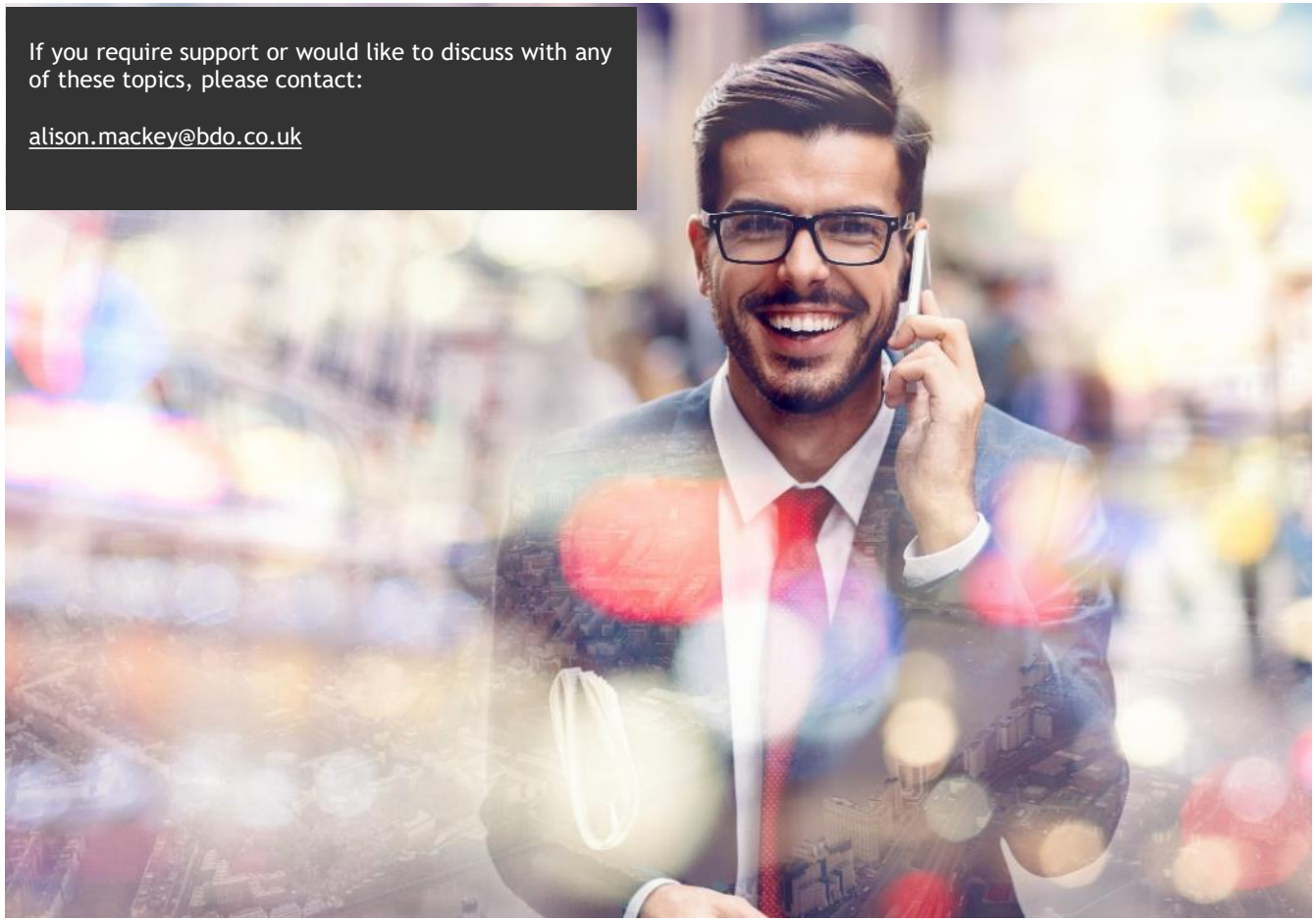
How can BDO support you?

As we have an existing Behavioural Risk methodology and SME capability within our FS Advisory Internal Audit team, we can provide you with tailored support:

- Assessing the 'current state' within your Internal Audit team and prioritisation of any gaps identified;
- Behavioural risk deep dive reviews: to identify patterns of undesirable employee behaviours which impact a Firm's ability to achieve its strategic objectives.
- Behavioural risk effectiveness review: to support the assessment of operating effectiveness, where the Firm has identified processes and controls in relation to the three areas of the Topical Requirement. This review will assess the 'lived reality' of employees and support an opinion on how specific mechanisms/processes/controls are being used and experienced across the Firm.
- Training and knowledge-building: to embed understanding of the Topical Requirement and how your Firm might approach audit coverage of organisational behaviour.

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

alison.mackey@bdo.co.uk



Back to contents

Are you ready for Provision 29 of the new UK Corporate Governance Code?

For most, FY26 will be the first year of reporting the requirements of Provision 29 of the UK Corporate Governance Code 2024 (the "Code"), effective for periods starting on or after 1 January 2026. This provision requires the boards of an applicable firm to issue a declaration over the effectiveness of material financial, operational, compliance and reporting controls as at the year end. Where there are instances of ineffectiveness this will need to be reported as well along with remedial actions taken.

Alex Traill
Director

alex.traill@bdo.co.uk

The financial services sector, particularly in the UK, is well known for its robust regulation and sophisticated understanding of risks and controls. Alongside this, the existing Code requires boards to review and monitor material controls (albeit without a formal declaration), so it is unsurprising that the Financial Reporting Council ("FRC"), the author of the new Code, does not see this enhancement as a substantial uplift. However, why are so many firms struggling to grapple with it? In this article we'll explore why this might be the case and make suggestions of how to overcome the challenges that persist.

Understand the existing provision

Undoubtedly the amendments to Provision 29 have been the most talked about change to the Code and have caused the most debate. Parties to these lively debates often need reminding of the existing requirements to review and monitor material controls. When challenged on the process and reporting in place to support existing disclosures in the annual report there is typically an air of uncertainty or, at the very least, a description of incohesive assurance activities.

Regardless of one's role in the business, be it on the board, part of the operations team or one of the three lines of defence, it is important to set out a solid foundation of understanding to ensure everyone knows the current requirements, where there may or may not be gaps and what the new requirements mean in the context of this newly established baseline.

Project plan and governance

Provision 29 requirements have stirred confusion among financial institutions, often due to a misplaced confidence stemming from their highly regulated environment. Many assume that existing measures already address these requirements, but this isn't necessarily the case in reality. A firm's regulatory environment will certainly play a role and will have established an undercurrent of controls in the business, but a fresh perspective is required to ensure Provision 29 is being addressed at the right level and not adopting an approach which is overly granular or burdensome to the business.

Determining a board level owner and establishing project and reporting governance is key to ensuring that the right level of work is being done to satisfy not only the requirements but also the board's appetite. Afterall, the board will be responsible for the declaration, so it is only right that they set the tone and direction of travel.

Setting an approach and understanding the risk profile, I recall hearing "This is not US SOX" on many occasions in the initial publicising of the FRC's changes to the Code. It is fascinating therefore to see so many firms adopting this level of granularity without stepping back to reflect on the true purpose of Provision 29.

continued >

Back to contents

Are you ready for Provision 29 of the new UK Corporate Governance Code?

The principled nature of the Code permits boards to set out an approach which is relevant to their business and gives the readers of the disclosures in the annual report a truly valuable understanding of the risk management and internal controls without the firm.

Setting this out earlier and promoting continuous engagement with the board is key to delivering an outcome which will be powerful in disclosure but not overly onerous or costly. Many firms have also used this moment as an opportunity to revisit principal risks and revise their risk taxonomy to ensure it truly reflects the current environment in which the firm operates.

Material controls

As already mentioned, the concept of material controls is not new. Therefore, in theory, firms should already be aware of their inventory of material controls and what work is being done under the existing Code to review and monitor these.

Where this is not the case, it is imperative to establish mechanisms to identifying material controls, reflecting on what materiality means to the board both from a quantitative and qualitative perspective and taking into account financial, operational, compliance and reporting controls. Many associate materiality with a numerical calculation, however, a more intuitive way of looking at Provision 29 controls may be to think about which controls are fundamentally critical to the business's performance and/or success.

One way to look at it (and there are many) may be that a control failure may have led to stakeholders changing their decision around doing business with or investing in the firm.

Current understanding of control environment

Is it possible to identify material controls without understanding key processes and systems and the wider control environment? This is another challenge to applicable firms and the documentation that it is expected from listed businesses around business processes and IT systems. Many have pockets of documentation which do not extend across the business in a consistent manner. The approach for Provision 29 will drive any additional work required in enhancing documentations but it is arguable that a suite of formal process documentation (perhaps in the form of process maps and/or risk and controls matrices) provides a solid foundation on which to identify truly material controls.

Assurance activities - strategy and approach (what's enough and by whom)

The Code does not make explicit mention of assurance over material controls. However, the requirement to carry out a review and issue a declaration is driving many boards to building an assurance plan that gives them the comfort they need. Assurance can be sought through a combination of risk and controls self-assessments, traditional controls testing through the first and second lines and/or specific audit work undertaken by the third line, as well as being both internally and externally sourced.

As a result of periodically introduced regulation, controls have been layered into a business for a specific purpose, often without much consideration of what already exists. These controls are also often accompanied by assurance frameworks run by different parts of the business resulting in an uncoordinated and inefficient assurance regime.

Provision 29 provides the opportunity to step back from the detail and reflect on what are the best combined assurance practices to meet multiple existing purposes as well as the board's internal control declaration. By-products of doing this will be streamlined activities, reduced pressure on the business and significant cost savings.

Navigating the complexities of Provision 29 requires a clear understanding of existing controls and a strategic approach to governance and assurance. While the financial services sector is accustomed to robust regulation, the new Code challenges firms to reassess their control environments and assurance activities. By establishing a board-level owner and promoting continuous engagement, firms can set a relevant approach that aligns with their risk profile and business needs. This is not about adopting a US SOX-like granularity but rather about ensuring meaningful disclosures that reflect the true purpose of the Code. Embracing this opportunity can lead to streamlined processes, reduced business pressure, and significant cost savings, ultimately enhancing the firm's performance and stakeholder confidence.

continued >

Back to contents

Are you ready for Provision 29 of the new UK Corporate Governance Code?

How can BDO support you?

As part of our continued commitment to supporting strong governance in the listed funds sector, we are pleased to introduce our Provision 34 readiness assessment – developed specifically to support boards in preparing for the new requirements under the AIC's updated Corporate Governance Code.

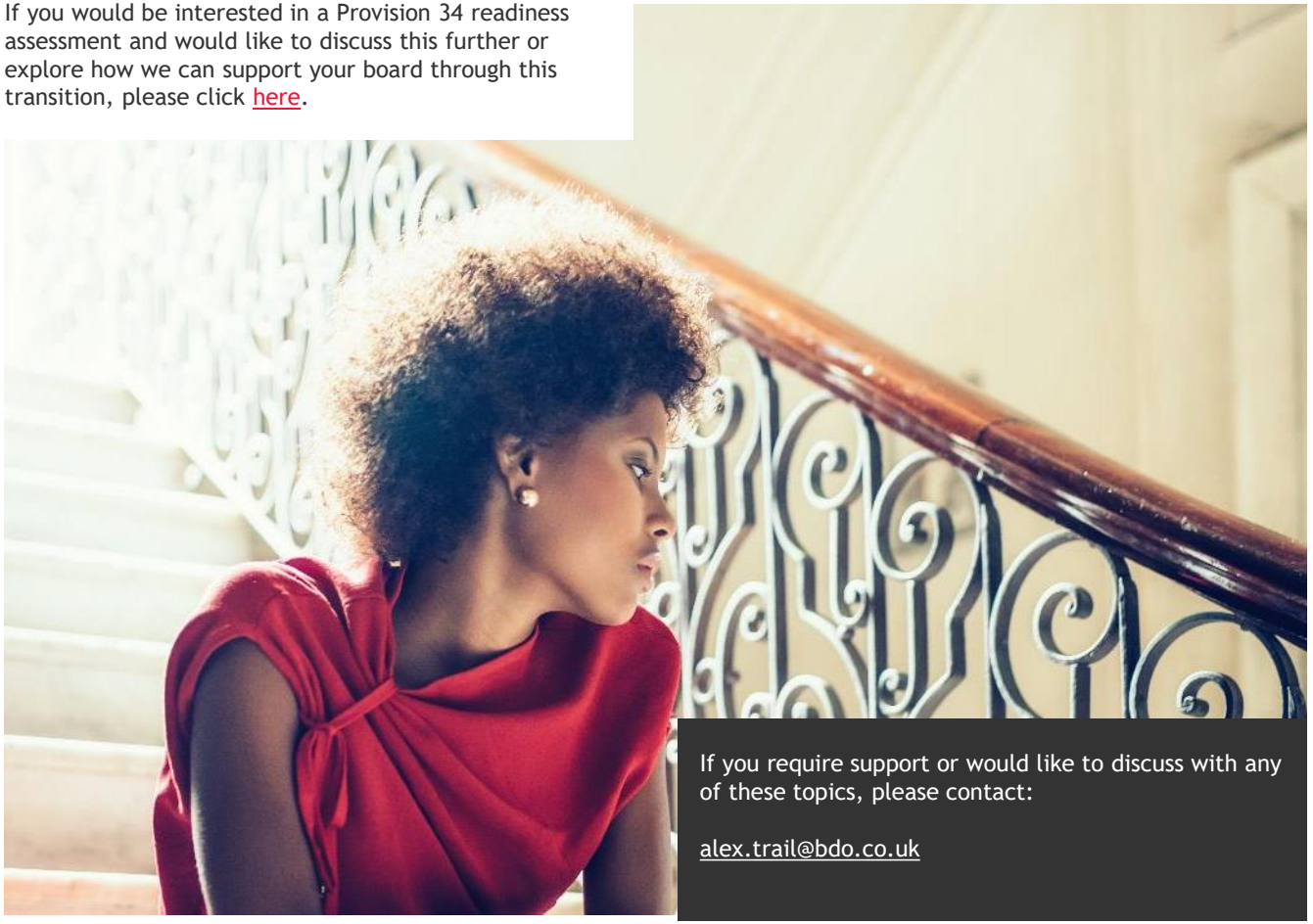
Provision 34, which comes into effect for accounting periods starting on or after 1 January 2026, introduces a requirement for boards to provide a formal declaration on the effectiveness of material financial, operational, reporting, and compliance controls. While many boards will already be undertaking activities aligned with this provision, our recent discussions suggest that confidence in current arrangements varies – particularly in how these align with the new expectations.

Our readiness assessment has been designed to:

- Provide a clear view of your current position against both existing and upcoming requirements
- Identify areas where enhancements may be appropriate
- Deliver a pragmatic roadmap towards achieving a successful declaration under Provision 34.

In line with our professional independence obligations, we are unable to offer this readiness assessment to our audit clients. However, for those we can support, this assessment can provide valuable early insight and help shape a proportionate and effective response ahead of the 2026 implementation date.

If you would be interested in a Provision 34 readiness assessment and would like to discuss this further or explore how we can support your board through this transition, please click here.



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

alex.trail@bdo.co.uk

Back to contents

Is HMRC's progress in tackling error and fraud in R&D claims actually a success?

BDO has taken a detailed look at the latest statistics on R&D tax relief claims published on 17 July 2025 in HMRC's annual report, with a particular focus on the impact of the Mandatory Random Enquiry Programme (MREP). The findings show significant progress in reducing error and fraud, but there are still areas that need improvement.

Whilst the Financial Services sector is not specifically noted by HMRC as having high levels of non-compliance, an awareness of HMRC's approach to R&D tax relief compliance is welcome in the context of the quantum and value of claims made by FS businesses.

Carrie Rutland
Head of FS R&D

carrie.rutland@bdo.co.uk

Romane Reeves
Associate Tax Director

romane.reeves@bdo.co.uk

HMRC's publication of their estimates of the amount of error and fraud in R&D tax relief claims in 2020 to 2021 drew much coverage and drove HMRC's actions to counter the loss of tax, including the recruitment of hundreds of additional R&D staff. At that time, the estimate was that the overall level of fraud and error was 16.7% (£1.13 billion). Most of this non-compliance was estimated to be in the SME R&D scheme.

At that time, HMRC risk-profiled claims across the different business sectors and by size of claim. It was estimated that only 41% of R&D claims made by SME businesses in the Financial Services sector were fully compliant, 41% were partially non-compliant and 18% of claims were non-compliant.

HMRC's approach to R&D tax relief claims has evolved since that time with significant policy and operational changes. They have also implemented the MREP Programme as part of their compliance approach.

Key R&D Findings from HMRC's annual report:

- Expenditure on R&D reliefs for 2024 to 2025 was £8.2 billion, supporting innovative projects in science and technology. Whilst this wasn't split by sector, R&D reliefs continue to have significant take up by the Financial Services sector
- HMRC processed 90% of claims within 40 days, surpassing their target of 85%
- The error and fraud rate for 2024 to 2025 was reduced to 5.9% (£481 million) overall, and 10.6% (£339 million) for the SME scheme
- This marks a decrease from previous years, with 2022 to 2023 estimated as 14.7% (£652 million) for the SME scheme and 3.3% (£107 million) for RDEC
- Compared to 2020 to 2021, the overall amount of error and fraud is estimated to have fallen by £649 million.

Impact of the MREP Programme:
The MREP programme has played a crucial role in HMRC's efforts to tackle fraud and error in R&D claims. By enhancing scrutiny and verification processes, the programme has helped ensure that claims are legitimate and that the system's integrity is maintained. The programme's focus on collaboration with industry experts has refined claim assessments, leading to more accurate evaluations and reduced error rates.

BDO's view:
In our view, while HMRC has made strides in reducing fraud and error, we believe there is room for further improvement. The introduction of uniform R&D claim reporting via the Additional Information Form and increased, risk-based compliance activity are positive steps, but more robust measures are needed to ensure the integrity of the R&D tax relief system.

continued >

Back to contents

Is HMRC’s progress in tackling error and fraud in R&D claims actually a success?

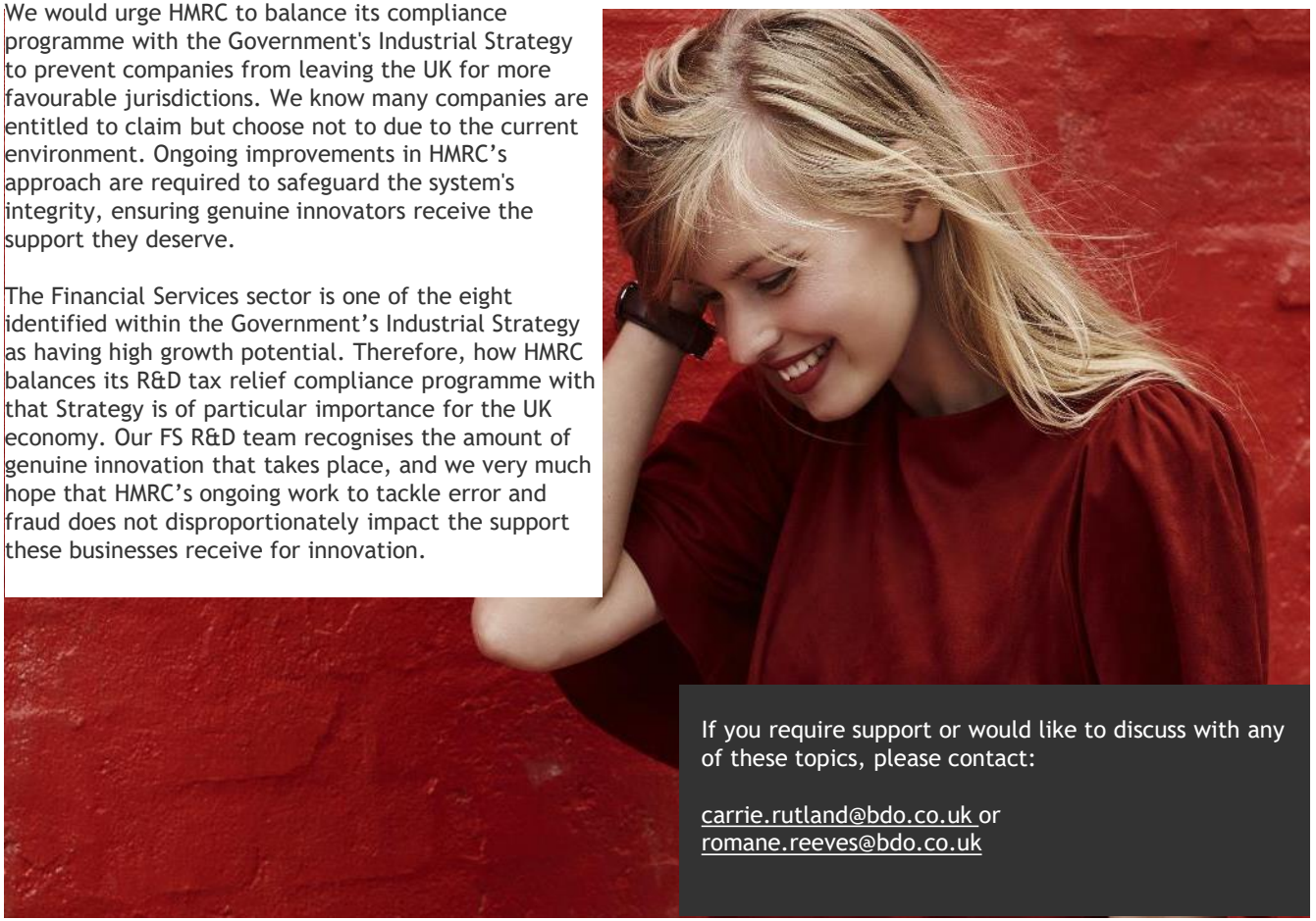
We recommend HMRC consider the following in relation to their approach to R&D tax relief claims in the future:

- Continued enhancement of scrutiny and verification processes to ensure claims are legitimate
- Greater consultation with industry experts when reviewing claims and implementing changes
- Increased transparency in reporting fraudulent claims to build trust in the system
- Careful debate on the introduction of an Advance Clearance Facility so that this brings about positive customer experience and greater compliance.

We have a concern that HMRC's recent compliance approach may be too heavy-handed, potentially discouraging legitimate claims, especially for smaller claimants. The methodology used in HMRC's statistical analysis could overstate error and fraud estimates, as it assumes all corrections arise from error or fraud. Many claimants abandon claims due to the resource demands of defending them, which should not be counted as fraud or error. The Additional Information Form, while mitigating error and fraud, imposes significant costs on companies, with larger groups facing extensive disclosure requirements. The original Impact Assessment outlining costs for this form was also flawed, ignoring the time needed to compile information.

We would urge HMRC to balance its compliance programme with the Government's Industrial Strategy to prevent companies from leaving the UK for more favourable jurisdictions. We know many companies are entitled to claim but choose not to due to the current environment. Ongoing improvements in HMRC’s approach are required to safeguard the system's integrity, ensuring genuine innovators receive the support they deserve.

The Financial Services sector is one of the eight identified within the Government’s Industrial Strategy as having high growth potential. Therefore, how HMRC balances its R&D tax relief compliance programme with that Strategy is of particular importance for the UK economy. Our FS R&D team recognises the amount of genuine innovation that takes place, and we very much hope that HMRC’s ongoing work to tackle error and fraud does not disproportionately impact the support these businesses receive for innovation.



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

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

Back to contents

FCA CP25/18: Tackling Non-Financial Misconduct in Financial Services

On the 2nd of July 2025, the Financial Conduct Authority (FCA) published Consultation Paper CP25/18 outlining new rule changes and proposals to address non-financial misconduct (NFM) in financial services. This further reinforces the regulatory standpoint that workplace behaviours such as bullying, harassment and violence can signal deeper cultural failings and can ultimately lead to consumer harm, poor market conduct and reputational risks.

Sasha Molodtsov
Partner

sasha.molodtsov@bdo.co.uk

Jennifer Cafferky
Associate Director

jennifer.cafferky@bdo.co.uk

Background and Context

On September 2023, the FCA published Consultation Paper (CP) CP23/20, which proposed a new regulatory framework on Diversity and Inclusion (D&I). The CP also included proposals to "clarify and strengthen" expectations around NFM.

Whilst the FCA publicly announced on the 12th of March 2025 that it would not be taking forward its D&I proposals (following further consideration of its cost benefit analysis (CBA)), NFM has remained firmly on the agenda.

The FCA's NFM proposals gained strong support during the D&I consultation period, and most respondents agreed that NFM was a regulatory issue, and 80% of authorised firms supported the FCA's proposed approach. The Treasury Select Committee (TSC) also welcomed more robust regulation in this area.

Summary of the Paper

There are two key elements to CP25/18:

- A Policy Statement extending the scope of Code of Conduct (COCON) to cover serious NFM in non-banks, aligning with the rules for banks and bringing more incidents into the scope of COCON
- A Consultation on additional guidance for firms to interpret and apply rules consistently, particularly for COCON and FIT (Fit and Proper test for Employees and Senior Personnel Sourcebook).

CP25/18 applies to all FSMA (Financial Services and Markets Act) firms with Part 4a permission and staff in those firms who are subject to COCON. The implementation date for expanding the scope of COCON is 1 September 2026, and consultation closes on 10 September 2025 with finalised guidance expected before the end of this year.

Policy Statement: Code of Conduct (COCON)

Currently, there is an inconsistency between rules that apply to banks and non-banks. Whilst the scope of COCON is relatively wide for banks, for non-banks COCON applies primarily to conduct relating to the SMCR financial activities of the firm.

In CP23/20, the FCA proposed to change the scope rules for non-banks to make bullying, harassment and similar behaviour between staff subject to the wider scope rules that apply to banks. With strong support for the proposal, the FCA has now confirmed it will widen the COCON scope rules for non-banks to align the approach across all SM&CR firms and bring more instances of NFM into scope.

As referenced above, the new rule comes into effect on 1 September 2026. This change will not apply retrospectively.

continued >

Back to contents

FCA CP25/18: Tackling Non-Financial Misconduct in Financial Services

Overview of proposals for consultation

CP25/18 also sets out proposals for potential new FCA Handbook guidance in COCON and FIT. The purpose of the guidance is to make it easier for SM&CR firms to interpret and consistently apply the conduct rules, and to clarify statutory and FCA requirements for fitness and propriety. The FCA is seeking views on whether additional guidance is needed and on the form any such guidance should take.

COCON guidance

New guidance on the scope of COCON, including guidance and examples of:

- The boundary between work and private life
- When conduct is outside of a firm's SM&CR financial activities
- When NFM may be out of scope as it relates to a non-financial services business of a firm
- Breaches of Individual Conduct Rule 1 (integrity) versus 2 (due skill, care and diligence)
- Factors to consider in determining whether NFM is serious enough to constitute a breach
- "Reasonable steps" for Managers to protect staff against NFM.

FIT guidance

Draft guidance on how various types of conduct, including NFM, are relevant to the FIT section of the FCA Handbook. This includes:

- Regulatory breaches
- Conduct connected to work
- Behaviour in private or personal life
- Social media and employee monitoring
- Relevant to competence and capability.

Proposals not being taken forward

The FCA also confirmed that it would not be progressing its proposals to:

- Extend the guidance on the Suitability Threshold Condition (in its COND Sourcebook) to make it clear that NFM is relevant to its assessment of firms' suitability to undertake regulated activities
- Update its guidance around regulatory references (in SYSC) to clarify that it might be necessary to provide information on NFM or misconduct outside of work as part of regulatory referencing.

What actions do firms need to take?

In response to CP25/18, firms should:

- Review current COCON policies and map against the proposed broader scope for serious NFM. Whilst the extension of the rules apply to non-banks, banks should also gain assurance that their policies align to regulatory expectations
- Review broader speak-up channels (including Whistleblowing and grievances frameworks) and culture to ensure alignment with regulatory expectations
- Assess disciplinary and conduct breach reporting frameworks to ensure consistency with the rule changes. Again, whilst this is primarily relevant for non-banks, this change serves as a prompt for banks to ensure that their arrangements are fit for purpose
- Prepare training plans to ensure staff understand the new expectations. Refresher training should also be considered for banks
- Respond to the FCA consultation, by 10 September 2025, using the online response form
- Monitor for the final guidance publication by the end of 2025 and ensure that the updated rules have been implemented ahead of the 1 September 2026 deadline.
- Download Non-Financial Misconduct Rules Preparation Checklist

continued >

Back to contents

FCA CP25/18: Tackling Non-Financial Misconduct in Financial Services

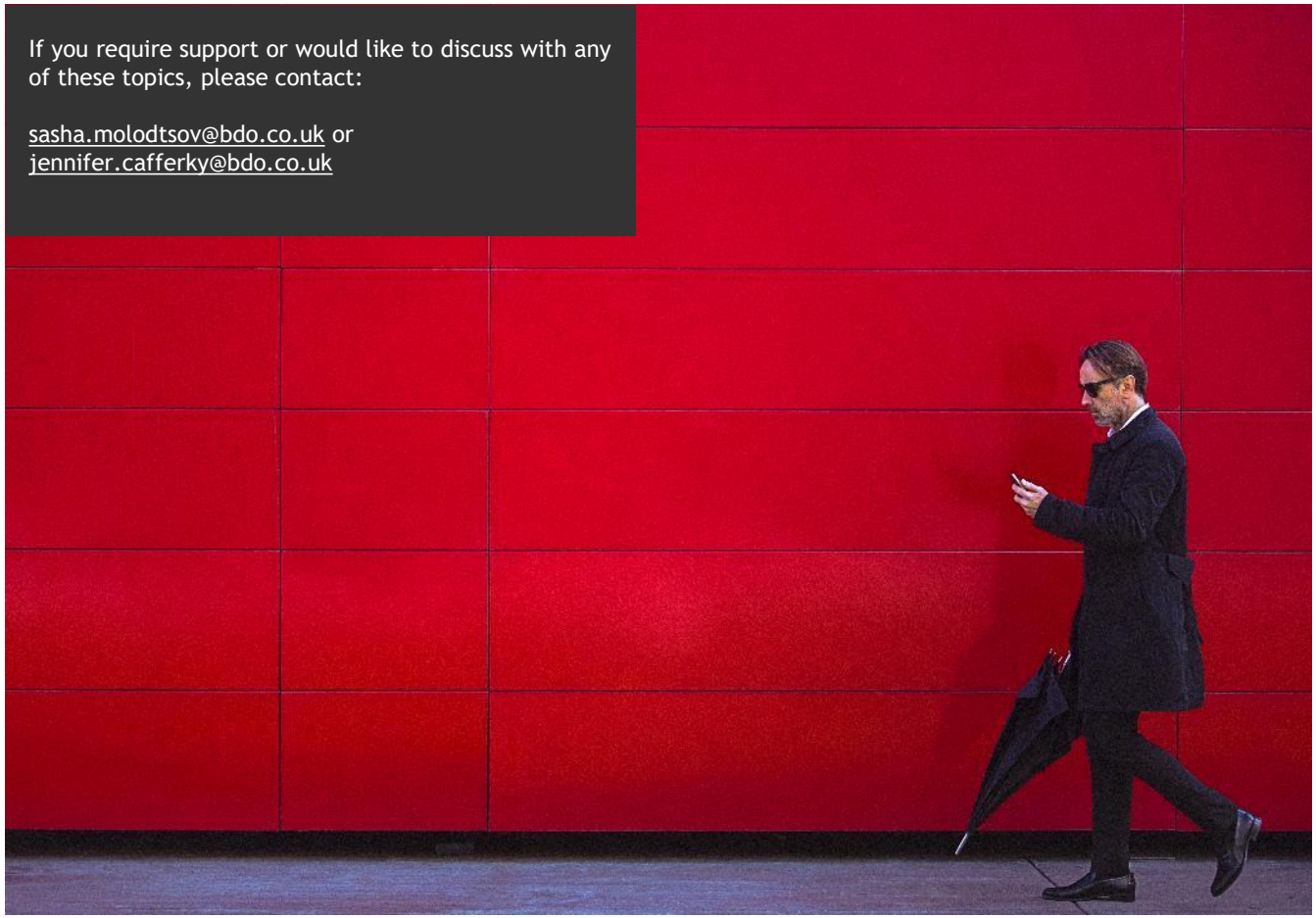
How can BDO support you?

Need help unpacking or implementing the changes? BDO can support you with:

- Assessing current COCON and FIT frameworks to identify gaps against new rules and proposed guidance
- Mapping the impact of the new rules on your policies, procedures and frameworks
- Reviewing your speak up arrangements and culture to identify potential risk areas
- Developing and delivering targeted training for Boards, Senior Managers, Certification Staff, HR and Compliance teams, and wider staff to embed understanding of the new COCON scope and rules.

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

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



Back to contents

The FCA updated expectations on Climate-related reporting timings for asset managers, life insurers and FCA-regulated pension providers

Asset managers, life insurers, and FCA-regulated pension providers face the challenge of navigating multiple sustainability disclosure regimes, including the FCA's TCFD rules. The FCA's updated requirements now allow firms to integrate TCFD and SDR reporting, enabling them to link TCFD reports within their sustainability reports.

Gloria Perez-Torres
Associate Director, FS Advisory

gloria.pereztorres@bdo.co.uk

Asset managers, life insurers and FCA-regulated pension providers, are required to report under multiple sustainability disclosure regimes and they have to consider the FCA's TCFD rules. Subject to assets under management and/or administration thresholds, these firms must make mandatory disclosures on an annual basis at entity and product level:

- Entity level: An annual TCFD entity report published in a prominent place on the main business website. This must set out how the firm take the climate into account in managing or administering investments on behalf of clients and consumers
- Product level: Disclosures (including a core set of climate metrics) on the firm products, and portfolios. The product level reports must be made in a prominent place on the main business website and be included or cross-referenced in an appropriate client communication, or made upon request to certain eligible institutional clients.

Under these rules, firms are also required to take reasonable steps to ensure their climate disclosures reflect TCFD Guidance, which makes recommendations on transition plans.

What is new

The FCA received feedback that the rules were too granular and as a result the FCA have updated the requirements to simplify and streamline sustainability disclosures.

FCA's updated requirements allow the interaction between TCFD and SDR reporting including both the content of the sustainability report and the timing of reporting. Firms can now link their TCFD reports within their sustainability reports and can meet TCFD rules within the SDR reports as one report.

What firms should consider

- A large firm (>50bn AUM) in scope of SDR can align reporting periods to produce a single report by June 2026. Until then, two reports are needed in 2025: (1) A TCFD report by 20 June and (2) An SDR report by 2 December (with TCFD disclosure linked or included). From 2026, firms may issue one aligned report by 30 June each year
- The FCA rules allow the repurpose of existing reports as long as they meet the SDR entity level rules, but firms must submit waiver requests for individual cases
- Additional work is planned by FCA to streamline and enhance sustainability reporting by simplifying disclosure rules to ease burden on firms, helping investors with accessible and decision-useful information, promoting international alignment and support UK's position as leader in sustainable finance.

continued >

Back to contents

The FCA updated expectations on Climate-related reporting timings for asset managers, life insurers and FCA-regulated pension providers

Other reporting considerations

In H1 2025, the FCA carried out a review of TCFD reporting among asset owners and managers through desk research and industry engagement. A summary of the findings and their next steps, will be published in H2 2025, including updates on the interplay between TCFD and SDR entity-level disclosures.

Firms should consider the FCA's feedback - published in their landing page on 8 August 2025 - which outline key barriers to TCFD Implementation, as follows:

- Data availability especially on forward-looking metrics like scenario analysis and climate value at risk
- Data comparability due to variations in methodologies for scenario analysis, which affected the comparability of reports between different firms
- Proportionality as some reports were highly technical making them complex for retail investors to engage with
- Accessibility to product reports were difficult to find, contributing to lower engagement levels from retail investors.

Firms will benefit from broadening their understanding on how this barriers are impacting their reporting as well as potential early actions they can take to mitigate them.

Next steps

Asset managers, life insurers, and FCA-regulated pension providers (as well as other in scope firms) can now consider how to take advantage of the reporting flexibility. This includes planning adjustments needed on the content and timing of their TCFD and SDR reports they should determine whether and how to align their disclosures.

The FCA is planning to take into consideration also the wider landscape, including the implementation of the UK Sustainability Reporting Standards (UK SRS) which will implement Sustainability Standards 1 and 2 by the International Sustainability Standards Board (ISSB) as well as strengthening their expectations on transition plan disclosures in line with the Transition Plan Taskforce framework.

What does this mean for firms

With the rise in greenwashing cases and increasing regulatory demands, there's a growing need for assurance in sustainability reports. Internal Audit teams are ideally placed to support the business by reviewing plans and controls to ensure they meet regulatory requirements and stakeholder expectations. This is a key advantage firms should utilise, as third line of defence teams possess unique insights into the firm's business model and strategy.

Wherever you are in the process of developing your TCFD and SDR disclosures, BDO can help you. Our Financial Services ESG team provides specialist ESG risk and regulatory advice to clients, providing support to firms in respect of ESG strategy, risk management arrangements, as well as related wider sustainability disclosures.

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

gloria.pereztorres@bdo.co.uk

Back to contents

UK Cyber Security & Resilience Bill – what financial services firms need to know

The Cyber Security and Resilience Bill will raise the UK's cyber resilience baseline to be more in line with the European Union's Network and Information Security 2 (NIS2) Directive and the Digital Operational Resilience Act (DORA).

For Financial Services firms, already regulated by the Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA), this represents alignment rather than a fundamental shift. The Bill expands scope to cover Managed Service Providers (MSPs), suppliers, and parts of Critical National Infrastructure (CNI).

It is important to caveat that the full content of the Bill is not yet known; these expectations are based on the UK Government's policy statements.

Vidya Tarun
Senior Analyst

vidya.tarun@bdo.co.uk

The Evolving Cyber Regulatory Landscape

Cyber security has long been a priority for UK regulators and industry leaders, but the regulatory environment is undergoing a significant transformation. This shift is driven by the increasing sophistication of cyber threats, the expanding interconnectivity of critical sectors, and the recognition that cyber resilience is fundamental to economic growth.

Financial Services Perspective

Financial Services (FS) firms already operate under robust regulatory expectations, including the Prudential Regulation Authority (PRA) operational resilience rules, the Financial Conduct Authority (FCA) cyber and technology risk management expectations, and for cross-border entities, the EU's Digital Operational Resilience Act (DORA). Recent developments have broadened regulatory oversight to cover critical third-party service providers such as cloud and technology firms that support essential FS operations. Regulators now have enhanced authority to require incident reporting, gather information, and direct remedial actions for these providers, deepening the compliance interdependencies between FS firms and their supply chain.

UK Critical National Infrastructure Perspective

UK Critical National Infrastructure (CNI) spans sectors such as energy, water, transport, health, and digital infrastructure. In 2024, the government extended the definition to include data infrastructure recognising its central role in national service delivery.

These sectors are facing heightened risks from state-sponsored actors, organised crime, and the misuse of emerging technologies, including AI-driven attacks. In response, government investment has increased, including funding for initiatives such as a national Cyber Emergency Command to coordinate major incident responses.

Why the Landscape is Evolving

- Escalating threat levels: High-impact incidents affecting health services, retail groups, and FS demonstrate how quickly disruption can spread
- Interconnected risk: Outsourced IT, managed services, and cross-sector dependencies mean that a single failure can have system-wide consequences
- Economic imperative: Strong cyber security is now seen as a precondition for attracting investment, supporting innovation, and sustaining long-term growth.

What is the Cyber Security & Resilience Bill and When is it Coming?

Announced in the July 2024 King's Speech, the Cyber Security & Resilience Bill will modernise and expand the UK's Network and Information Systems (NIS) Regulations 2018. The Bill's Policy Statement (April 2025) outlines its scope, objectives, and timeline. It is expected to be introduced to Parliament later in 2025.

continued >

Back to contents

UK Cyber Security & Resilience Bill – what financial services firms need to know

Policy objectives include

- Driving economic growth by ensuring the security of essential infrastructure and the digital services that underpin it
- Expanding the remit of existing regulation to cover more sectors and entities
- Increasing incident reporting to improve government visibility of cyber threats
- Addressing specific UK cyber security challenges while aligning, where appropriate, with the EU's NIS2 Directive
- Strengthening supply-chain security obligations for operators of essential services (OES) and relevant digital service providers (RDSP).

Scope Expansions & Key Provisions

More entities in scope

- Managed Service Providers (MSPs), due to their deep access to client networks
- Data centres above defined capacity thresholds (designated as CNI in September 2024)
- Regulator-designated Designated Critical Suppliers (DCS).

Supply-chain duties

The Bill strengthens expectations around how organisations manage their suppliers and respond to incidents. Key changes include:

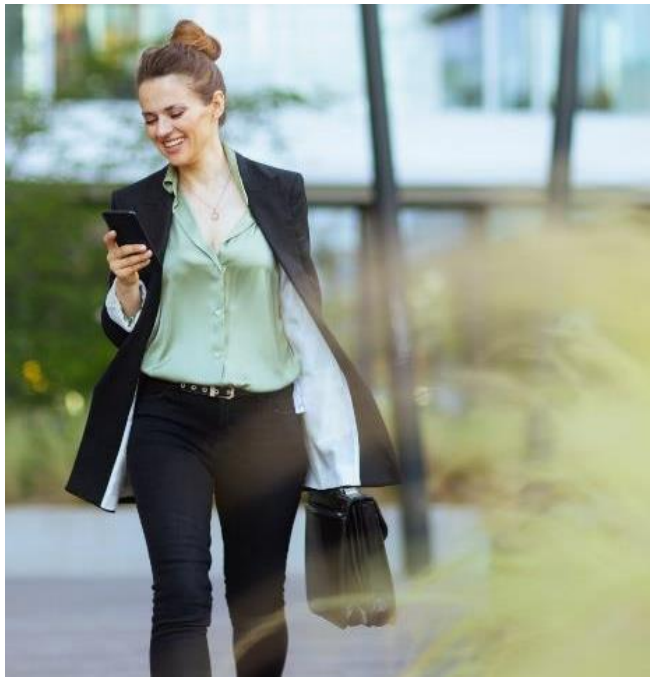
- **Supplier accountability:** Operators of Essential Services (OES) and Relevant Digital Service Providers (RDSP) must take clearer responsibility for identifying and managing risks across their supply chain
- **Faster incident reporting:**
  - Notify both the regulator and the National Cyber Security Centre (NCSC) within 24 hours of a major incident
  - Provide a full report within 72 hours
  - Reporting will now cover a wider set of impacts (confidentiality, integrity, and availability of systems) and attacks that come through third parties, such as Managed Service Providers (MSPs).

Regulatory Landscape Comparison

The Bill sits alongside other UK and EU regimes. The table below summarises their scope, focus, and sector coverage for quick references:

Wherever you are in the process of developing your TCFD and SDR disclosures, BDO can help you. Our Financial Services ESG team provides specialist ESG risk and regulatory advice to clients, providing support to firms in respect of ESG strategy, risk management arrangements, as well as related wider sustainability disclosures.

continued >



Back to contents

UK Cyber Security & Resilience Bill – what financial services firms need to know

Regulation	Scope	Focus	Sector Coverage
Cyber Security & Resilience Bill (UK)	Broadly targets cyber security across multiple UK sectors	Establishes comprehensive cyber security standards and resilience frameworks; integrates with existing operational strategies	Multiple sectors, including FS, CNI, healthcare, energy, transport, and digital infrastructure
DORA (EU)	Financial sector within the EU	Ensures financial entities can withstand and recover from ICT disruptions; stringent ICT risk management requirements	Banks, investment firms, insurance companies, and other regulated FS entities
PRA Operational Resilience (UK)	UK financial sector	Identifying and mitigating risks to operational resilience; sets impact tolerances and scenario testing requirements	PRA-regulated banks, insurers, and other deposit takers
NIS2 Directive (EU)	Essential and important entities across the EU	Enhances cyber security and resilience of network and information systems; strengthens risk management and incident reporting	Wide range of sectors, including energy, transport, health, water, and digital services
NIS Regulations 2018 (UK)	Operators of essential services and digital service providers in the UK	Ensures security and resilience of network and information systems; sets risk management and reporting requirements	Energy, transport, drinking water, health, digital infrastructure, certain digital services

What Does This Mean for UK Financial Services Firms?
While FS firms already operate under strong operational resilience and cyber requirements, the Bill introduces additional obligations that extend beyond current PRA and FCA rules.

Key Implications

- Third-party oversight: With MSPs now directly regulated, FS firms will need to revisit supplier contracts, due diligence processes, and monitoring frameworks to ensure alignment with new standards.
- Faster incident escalation: The 24/72-hour reporting model requires clearly defined detection, escalation, and regulatory communication processes.
- Cross-border compliance: The Bill's alignment with NIS2 and practical parallels with DORA will aid consistency for firms operating internationally, but jurisdictional nuances will require careful management.
- Integration with operational resilience: Cyber resilience requirements should be embedded into broader operational resilience frameworks, ensuring scenario testing and recovery plans reflect expanded threat criteria.

continued >

Back to contents

UK Cyber Security & Resilience Bill – what financial services firms need to know

Recommended Next Steps

1) Gap analysis – compare current controls with anticipated Bill requirements

2) Supplier risk review – prioritise MSPs, critical IT vendors, and potential DCS

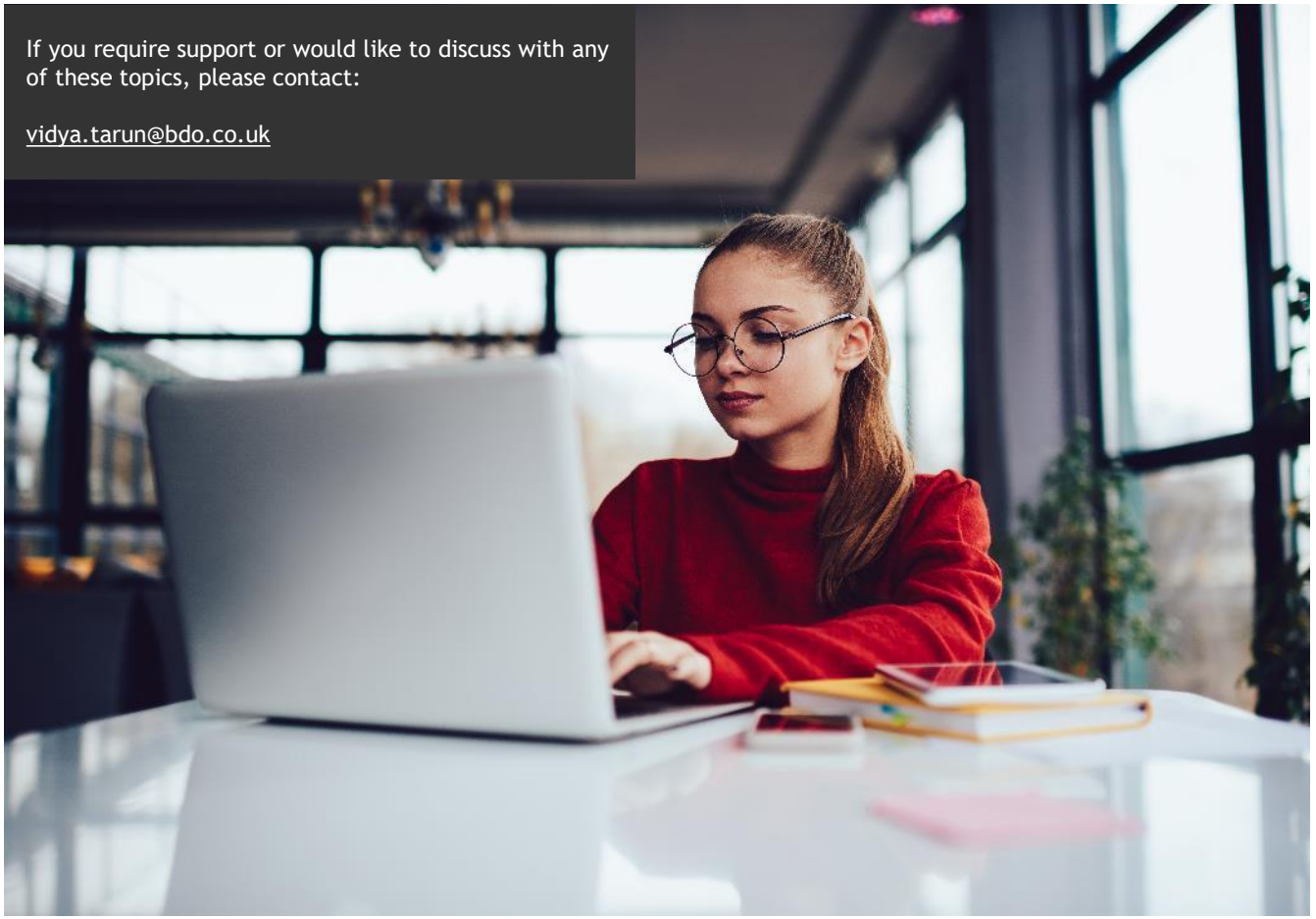
3) Incident reporting drill – simulate a 24-hour notification scenario

4) Regulatory engagement – maintain dialogue with sector regulators as implementation guidance emerges.

To conclude, the Bill signals a decisive step towards raising the UK's cyber resilience baseline. While details are still emerging, firms should act now to prepare by tightening supplier oversight, rehearsing faster incident reporting, and engaging with regulators to shape guidance.

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

vidya.tarun@bdo.co.uk



Back to contents

UK Corporate Governance Compliance: Why IT is now pivotal

Following the Financial Reporting Council's (FRC) update to the UK Corporate Governance Code, listed organisations will soon need to report on the effectiveness of their internal control framework, including IT aspects. This will be applied to organisations with a financial year starting on or after 1 January 2026. Through the Code there is an expectation that organisations maintain high standards of integrity and transparency in their reporting and operations, which extends to how IT systems capture, process and report data. Whether information is financial or non-financial, meant for internal purposes or external disclosures, it is recorded, processed, stored, communicated, and reported using digital technology. The digital era has transformed the way we approach compliance. Here we explore some of the areas where IT plays a key role in meeting an organisation's reporting and compliance objectives.

Lisa Erasmus
Director, BDO Digital

lisa.erasmus@bdo.co.uk

Internal Controls: Supported by IT

Strong processes and controls are underpinned by effectively controlled and monitored IT systems. Without understanding an enterprise-wide IT environment, it is incredibly difficult and expensive to demonstrate effective internal control over financial reporting, operational risk and compliance with relevant regulations. The intersection between IT controls, process controls and entity level is crucial in developing a holistic and efficient control environment to address material risk.

IT Governance: The Silent Guardian

IT governance can be the silent guardian of corporate governance. The strategic alignment of IT with corporate governance ensures that technology not only supports and enhances corporate governance frameworks and processes. IT has a key role to play in maintaining compliance with the principles set out by the UK Corporate Governance Code.

IT Risks: The Board's New Frontier

The need to identify and address IT risks is a new frontier for many organisations and their boards. Cyber threats, data breaches and technology failures can undermine the trust in organisations. Boards are now required to have a firm grasp of IT risks and ensure that appropriate controls are in place. This is to protect the organisation's digital assets, provide confidence over the financial statement as well as ensure that operational resilience is strong.

IT Compliance: A Strategic Imperative

IT compliance should embed regulatory requirements into IT and business operations. Enforcing a strong compliance culture and controls mindset into operations enables compliance with current regulations. It also helps organisations adapt to future regulatory requirements.

IT Dependency and Corporate reporting

The accuracy and reliability of data are heavily dependent on robust IT systems. From financial statements to Board and Director statements to Task Force on Climate-related Financial Disclosures (TCFD) reporting and Environmental, Social, and Governance (ESG) reporting, IT systems are the backbone that supports these critical functions.

The dependency on IT systems' accuracy and reliability for corporate reporting is one aspect of this issue. IT systems and the data they generate can also help identify trends, highlight risks and uncover opportunities to drive growth. All of which are crucial to achieving sustained business success.

continued >

Back to contents

UK Corporate Governance Compliance: Why IT is pivotal

How we can help you

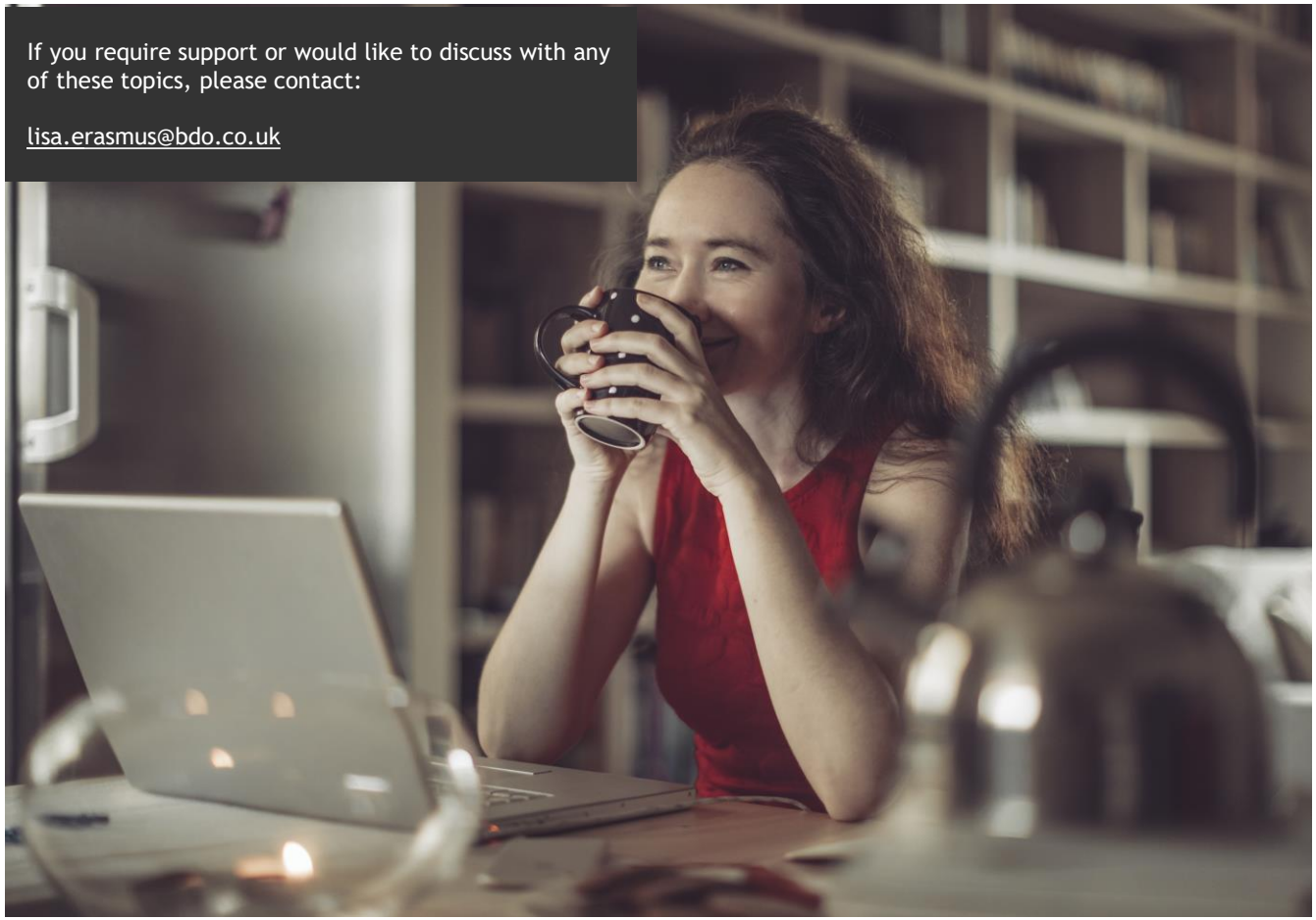
As digital technology becomes increasingly fundamental to how businesses operate, organisations must also recognise the strategic importance of IT in corporate governance. By integrating IT management into the fabric of corporate governance, organisations can not only meet the standards set by the FRC but also improve efficiency, resilience and ultimately, growth.

We have developed a simple, step-by-step approach to meeting the new corporate governance requirements and how they interact with your IT processes and technology stack. Compliance with other financial services regulations (such as FCA/PRA) should be leveraged when determining the approach for compliance to Code revisions, particular with respect to internal control.

Internal Audit can play a leading role in developing an assurance map to detail how existing regulation compliance can support Code compliance, as well as a controls gap assessment for IT and financial processes.

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

lisa.erasmus@bdo.co.uk



Back to contents

Strengthening CASS compliance: Why CASS internal audit matters

Those firms that hold client money and/or safeguard client assets will be subject to the FCA's CASS rules. While the FCA takes significant comfort from the annual external CASS audit, firms are expected to determine an appropriate and proportionate approach to CASS regulatory compliance, looking at how the "three lines of defence" operates effectively to do so.

The nature of the firm's business and the risk exposure and appetite for CASS will determine whether an internal audit review of CASS is undertaken every year or no less than once every three years.

James Steele-Perkins
Partner

james.steele-perkins@bdo.co.uk

The FCA continues to focus on CASS, closely examining firms' arrangements. Our insights highlight ongoing challenges such as maintaining accurate records, ensuring adequate organisational arrangements, and addressing reconciliation issues like unclear break narratives and misapplication of CASS rules. More broadly we see ongoing poor documentation and execution of controls at a time when the CASS rules have remained "steady state".

There are certain areas of CASS and other FCA associated rules (e.g. SUP for the monthly client money and asset return) where these are not externally audited and should be assessed.

CASS internal audits are vital in your firm's risk management framework, acting as the third line of defence. They offer an independent and objective view that complements the oversight provided by the first and second lines, as well as your external auditor. This helps pinpoint unnoticed weaknesses in processes, ensuring your firm remains robust and secure.

In today's regulatory environment, CASS internal audits are more than a compliance requirement—they are a strategic tool for CASS risk management and operational efficiency. Integrating these audits into your firm's governance arrangements keeps you vigilant, responsive, and ready to meet evolving regulatory demands. We can provide outsourced/co-sourced internal audit assurance in this specialist area.

We bring audit and consultancy expertise to the relationship, ensuring that team members interacting with senior management have real credibility along with the ability to add value through their industry expertise and experience.

Each firm and their needs are different, and it is therefore important that you engage with an advisor that can provide you with a tailored solution to meet your needs, address your risks and resolve challenges.

continued >

Back to contents

Strengthening CASS compliance: Why CASS internal audit matters

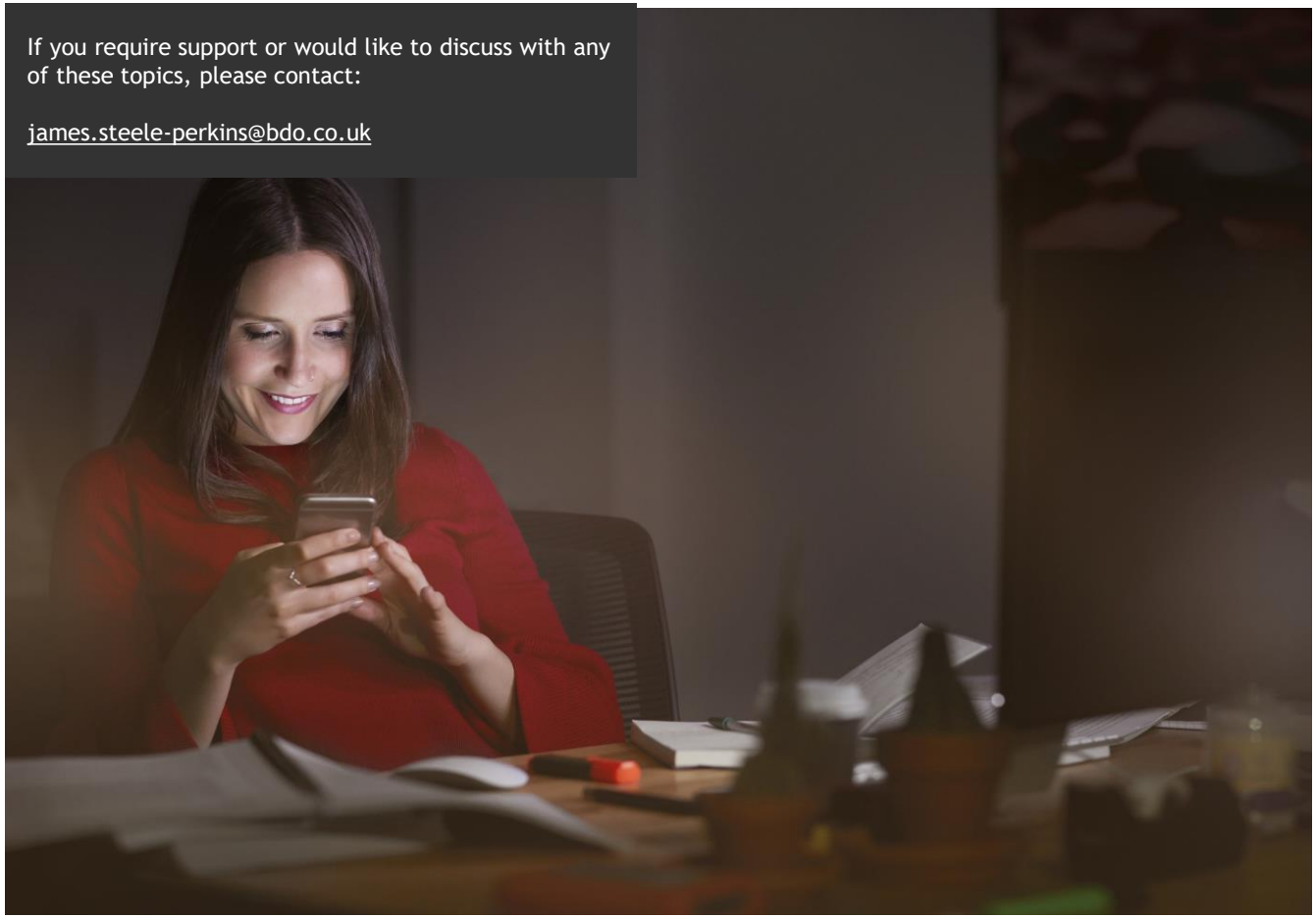
Examples of what we can offer:

- **Risk Assessment:** We help you identify and evaluate risks associated with your CASS compliance, ensuring you understand potential vulnerabilities, particularly at times or business or regulatory change
- **Process Review:** We examine your existing processes to ensure they align with CASS requirements, offering recommendations for improvements where necessary
- **Documentation:** We assist in reviewing and updating your documentation to ensure it meets regulatory standards and accurately reflects your processes
- **Training and Development:** We provide training sessions to enhance your team's understanding of CASS regulations and their application in your business
- **Testing and Monitoring:** We support you in implementing effective testing and monitoring systems to ensure ongoing compliance with CASS rules
- **Reporting:** We guide you in preparing clear and accurate reports for internal and external stakeholders, ensuring transparency and compliance
- **Remediation Plans:** If issues are identified, we help you develop and implement remediation plans to address them promptly and effectively.

Our goal is to deliver exceptional client service, ensuring you have the support you need to navigate CASS internal audits with confidence.

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

james.steele-perkins@bdo.co.uk



Appendices

Back to contents

Appendix 1: Hot topics mapped against CIIA Code requirements

To conform with Principle 8 of the Code, Internal Audit should include the following 12 areas within its scope. Below we map each the hot topic against these scope areas to help Internal Audit in addressing this requirement.

Scope area under Principle 8 of the Code	Hot topic section
1. Purpose, strategy and business model	02. ESG and sustainable finance (p 11) 08. Digital (p 38)
2. Organisational culture	02. ESG and sustainable finance (p11) 03. Culture and behavioural risk (p 19)
3. Internal governance	01. Corporate governance (p 9) 06. Tax governance (p 30) [Note: Generally covered through most scopes as they review firm governance structures relevant to the subject matter]
4. The setting of, and adherence to, the risks the entity is willing to accept (risk appetite)	01. Corporate governance (p 9) [Note: Generally covered through most rated reviews]
5. Key corporate and external events	01. Corporate governance (p 9) 02. ESG and sustainable finance (p 11) 07. Prudential (p 34) 09. Digital (p 48)
6. Capital and liquidity	07. Prudential (p 34)
7. Risks of poor customer treatment, giving rise to conduct or reputational risk	04. Consumer duty (p 22) 06. Financial crime (p 31) {05. Financial crime (p 25)}

Back to contents

Appendix 1: Hot topics mapped against CIIA code requirements (continued)

Scope area under Principle 8 of the Code	Hot topic section
8. Environmental sustainability, climate change risks and social issues	02. ESG and sustainable finance (p 11) 07. Prudential (p 34)
9. Financial crime, economic crime and fraud	05. Financial crime (p 25)
10. Technology, cyber, digital and data risks	08. Digital (p 38)
11. Risk management, compliance, finance and control functions	01. Corporate governance (p 9) 02. ESG and sustainable finance (p 11) 04. Consumer duty (p 22) 05. Financial crime (p 25) 06. Tax governance (p 30) 07. Prudential (p 34) [Note: Most topic areas cover either of the following functions – Risk Management, Compliance, Finance or control functions one of the following covered through most scopes, and most topic areas cover aspects of compliance, finance and control functions]
12. Outcomes of processes	[Note: Most scopes cover this requirement as they review firm policy and procedures relevant to the subject matter]

Back to contents

Appendix 2: Hot topics by section

Below is a list of the hot topics covered in each section of this pack.

Section	Hot topic area
01. Corporate governance (p 9)	UK Corporate Governance Code 2024
02. ESG and sustainable finance (p 11)	PRA's enhanced climate change risk management expectations for banks and insurers Greenhouse Gas (GHG) emissions and sustainability disclosures Taskforce on Climate-related Financial Disclosures (TCFD) ESG strategy and transition plans Anti-Greenwashing Rule (AGR) Sustainability Disclosure Requirements (SDR) and Naming and Labelling Regime Diversity and Inclusion EU Corporate Sustainability Reporting Directive (CSRD) Taskforce of Nature-Related Financial Disclosures (TNFD) UK Government consultations
03. Culture and behavioural risk (p 19)	Culture Behavioural risk
04. Consumer Duty (p 22)	Embedding the Consumer Duty regulation Product governance and fair value Vulnerable Customers
05. Financial crime (p 25)	Sanctions risk management Fraud risk management – ECCTA failure to prevent offence AML - transaction monitoring Fraud risk management – APP fraud Market abuse

Back to contents

Appendix 2: Hot topics by section
(continued)

Section	Hot topic area
06. Tax governance (p 30)	Senior Accounting Officer ('SAO') compliance Failure to Prevent Tax Fraud – CCO and FTPF Tax Control Framework and operating effectiveness
07. Prudential (p 34)	Liquidity Assessments within the ICARA Regulatory Reporting (Prudential) Transaction Reporting (MIFIR and EMIR) Risk Management Wind-down planning
08. Digital (p 38)	Cyber Security Cloud environments Outsourcing and third parties Resilience Artificial Intelligence IT change programmes Data governance Payments Review (SWIFT/Faster Payments) IT governance IT general controls

FOR MORE INFORMATION:

Chris Bellairs
Partner

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

Bruk Woldegabreil
Director

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

Sam Ewen
Manager

+44 (0)7570 728790
sam.ewen@bdo.co.uk

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

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

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

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

Copyright © 2025 BDO LLP. All rights reserved. Published in the UK.

www.bdo.co.uk