2025 Horizon scanning for assurance functions

Asset and wealth management

September 2024

pwc

Nicole McManus
Partner
PwC UK Financial Services
Internal Audit Leader

M: + 44 (0) 7989 950485
E: nicole.r.mcmanus@pwc.com

In a world of increasing change and uncertainty, foresight is vital

In today's rapidly evolving business landscape, organisations face an array of unprecedented risks and challenges. Technological advancements, shifting customer expectations, macroeconomic and geopolitical instability and climate change demand strategic agility and robust risk management. Whilst these risks are not new, their interconnectivity and the speed of change brings new challenges to businesses. Our 27th Annual Global CEO ('Chief Executive Officer') Survey tells us that, in 2024, CEOs are increasingly concerned about the long-term viability of their organisations, with many taking steps to refine or reinvent their business models.

Internal audit's role in helping businesses to navigate these risks, find opportunities and provide real value to stakeholders has never been more important. Foresight is key, and internal auditors need to be able to identify the future risks that matter to help businesses navigate this complex risk universe. Having the right people with the right skills will foster a more strategic focus. However, to be truly successful, functions will need to go beyond having the right skills, people and tools, and fully embed a culture and behaviours that encourage an innovative, growth mindset across the entire team.

The supervisory and regulatory agenda continues to be exceptionally busy as regulators and other policy makers respond to a range of macro-trends. Key legislative changes that will impact the year ahead include: The Financial Services and Markets Act ('FSMA') 2023, the Edinburgh Reforms and updates to the UK Corporate Governance Code. Furthermore, the Government has outlined its vision for a financial sector that aims to balance consumer protection, competitiveness, innovation and financial stability.

This year, our document covers the following areas:

- **Macrotrends:** This sets out the latest UK economic outlook and geopolitical risks.
- **Regulatory landscape:** This covers key regulatory updates such as an overview of the UK regulatory agenda, changes to the UK's Corporate Governance Code, the annual business plans from the regulators.
- **Risk hot spots:** We deep dive into six key hot spots that are impacting FS and are at the forefront of boardroom discussions: (i) Conduct and governance, (ii) Prudential matters, (iii) Digital assets, (iv) Technology and operations, (v) Financial crime and (vi) Environmental, social and governance ('ESG'). Whilst these hot spots are mostly consistent with the previous year, we have included new and contemporary topics under each of the hot spots and in some cases expanded on existing topics.
- **Professional Practices Standards**: This covers the key changes to the Institute of Internal Auditors (IIA's) Global Internal Audit Standards and provides an overview of the Chartered Institute of Internal Auditors ('CIIA')'s newly published, combined Internal Audit Code of Practice, which will both be effective from January 2025.

We hope this paper acts as a useful reference for you and, should you wish to discuss any aspect further, please do not hesitate to contact me or one of my colleagues whose contact details are at the end of this paper.

PwC 27th Annual Global CEO Survey 2024

Contents

01

Macro trends

- Geopolitical uncertainty
- UK economic outlook

Geopolitical uncertainty

In recent years, global events and geopolitics have shaped the risk environment - creating uncertainty and encouraging a focus on resilience.

The impacts of conflicts, economic challenges and political shifts feature heavily in the list of risks facing organisations in 2024, as the 'year of elections' continues. These sit alongside, and are compounded by, the rapid pace of technological change and its many impacts (on business, consumers, governments and criminals / hacktivists) and continued pressure from regulators, consumers and campaigners for action on climate change and the protection of our natural resources.

These interrelated and fast moving macro-risks affect consumer habits and expectations, operations and supply chains. Business leaders face considerable challenges in making sound decisions in the face of such complexity and uncertainty.

Organisational impacts

Risks driven by geopolitics will result in a wide range of impacts to business and organisations. Some of these will manifest in 2024, others will take longer to be felt, but are nevertheless worth considering now. Internal auditors need to be alert to the changing risk profile and its impacts on the control environment and organisational assurance needs. Based on the current geopolitical risk environment, below are several hypothetical scenarios that highlight how geopolitics could plausibly impact business.

Short-term scenarios (2024):

01

Increased supply chain disruptions: Conflict dynamics and political tensions in the Middle East, eastern Europe, and Asia expose organisations to supply chain disruption. Advanced technology, data, mineral resources, and semiconductors are especially exposed.

02

A focus on national resilience: Faced with vulnerability of critical inputs to acute shocks or malicious actions, many governments across the globe have taken short-term measures aimed at incentivising domestic resilience - whether through tariffs and protectionist policies or a focus on food and energy security, for example. For both governments and businesses, resilience is increasingly weighed against economic efficiency in decision-making.

03

A complex and changing environment for global business models: Driven by protectionism, changes to taxes, duties and tariffs, labour laws and sanctions impact both strategic decision making and day-to-day operations for global operators. Meanwhile, the drive for a focus on sustainable growth and protection of natural resources, has seen the development of a range of new reporting requirements.

Navigating the new landscape poses challenges to cross-border transactions, reputation, Environmental, social and governance ('ESG') management, and talent acquisition.

04

The geopolitical outlook drives heightened cyber risks: Cyber security has become part of the arsenal in geopolitical conflicts, and attacks can be sophisticated and persistent. Attackers often gain a foothold by stealing user credentials and then move unimpeded between systems. Attacks can spread around the world in hours rather than days thanks to automation. Multinational and global organisations can be affected even if they are not directly targeted.

05

Election results change the investment landscape: By the end of 2024, 75% of democratic countries will have held elections within the calendar year. New governments could invoke shifts in industrial strategy, trading relationships, regulations, and foreign policy, with implications for global competition. We anticipate some market repositioning as investment flows adjust to new conditions.

Geopolitical uncertainty (continued)

Medium-term scenarios (2025-27):

01

Impacts of protectionism filter through: Newly introduced protectionist legislation begins exhibiting impacts more forcefully, generating compliance challenges and risks to business operational models.

02

Global realignment of key powers following elections: Results of 2024 elections, notably the inauguration of the United States ('US') presidential election winner, the embedding of the new United Kingdom ('UK') government, and other results in key territories, lead to further trade legislation. Organisations will need to be resilient to withstand change and disruption and to respond with agility to new challenges and opportunities.

03

Geopolitical fault lines shape the competitive landscape: Scarcity of critical minerals, the desire to accelerate green technology advancements, and state-led protectionism over emerging technologies intensifies the competitive environment. The resources (i.e. raw materials, infrastructure development, and production capacity) of 'non-aligned' countries (those without a clear affiliation to an existing power-block) become increasingly contested. Businesses without plans for managing change become highly exposed.

UK economic outlook

Below, we summarise key points from our analysis of the UK economy, which focuses on UK growth outlook and inflation.

One of the new government's top priorities is to kickstart economic growth with the aspirational goal of achieving the 'highest sustained growth in the G7.' Assuming this strictly refers to economic growth rather than a broader measure of prosperity, our analysis indicates that this goal has not been achieved in decades. Additionally, the current government has committed to the previous government's fiscal rules to reduce debt as a share of Gross Domestic Product ('GDP'), and paired with tax cuts from the spring budget, the public purse is tight. The government could rely on three sources of growth: getting people back to work, implementing a robust industrial strategy to attract private investment, and leveraging technology more effectively to boost productivity. Given that the UK is expected to see very limited growth in its working-age population over the next decade, future growth must focus on increasing the capital stock of the UK economy and using existing resources more productively-areas where the UK has historically struggled. However, there is an opportunity to establish a new model of inclusive growth. The rise of Generative AI and the urgent need to transition to net zero present unique opportunities to drive this change. A key lever to initiate this transformation is committing to an industrial strategy.

01

UK inflation outlook

The worst phase of the cost of living crisis appears to be behind us, and economic activity is gaining momentum, defined by a 0.7% increase in Q1 2024 GDP, 11 consecutive months of real earnings growth, and a rebound in consumer sentiment to levels seen two years ago. Inflation is projected to hover around the 2% target for the rest of 2024. This volatility is due to a reduction in services inflation as the labour market cools, although rising energy prices, indicated by futures curves, suggest a slight uptick in overall inflation will be seen in October 2024, which may pose a challenge. Additionally, the Bank of England ('BoE') has initiated a rate-cutting cycle, though there remains some uncertainty regarding the pace of monetary loosening. Markets are currently anticipating an additional 35 basis point reduction by the end of the year 2024.

02

Labour market outlook

The Office of National Statistics continues to advise caution when interpreting labor market statistics due to the low response rate of the Labour Force Survey ('LFS'), which is set to be replaced by the Transformed Labour Force Survey ('TLFS') later this year. However, a broad suite of indicators provides strong evidence that the UK labor market is normalising, with unemployment and employment returning to pre-pandemic levels and vacancies down from their peak in June 2024 but still 11.6% higher than pre-pandemic levels. Economic inactivity remains a challenge, with 820,000 more working-age individuals not seeking work or unable to work compared to pre-pandemic levels, driven by long-term sickness and an increase of non-working students. Although labour demand has softened, vacancy rates in most sectors remain robust compared to pre-pandemic levels.

03

Corporate insolvencies

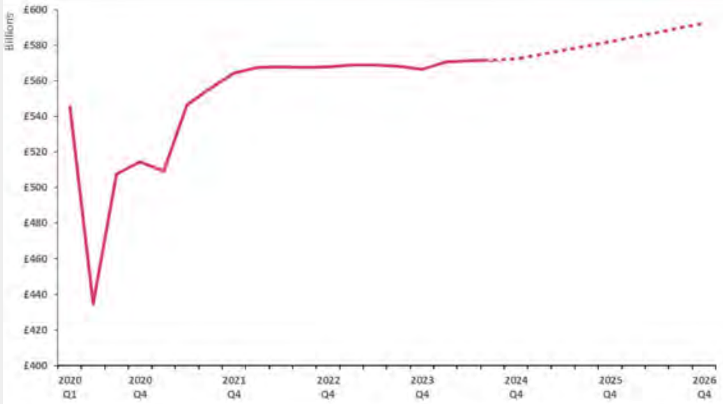
Corporate insolvencies in the UK reached nearly 27,000 in 2023, the highest level in over three decades and surpassing volumes seen during the global financial crisis. Despite this, the liquidation rate remains relatively low at 54 per 10,000 active firms. Initially, the increase in insolvencies was concentrated among smaller, micro firms, many of which were newly created during the pandemic by first-time entrepreneurs who typically hired few employees, held minimal debt, and relied heavily on government-backed loans. Econometric modeling predicts that corporate insolvencies will continue to rise, potentially reaching 30,000 by the end of 2024. The profile of insolvent firms is evolving, with larger firms and sectors such as wholesale and retail, construction, and hotels and catering increasingly affected by subdued demand, higher borrowing costs and elevated input costs.

UK growth outlook

This scenario projection suggests annual growth in UK GDP of 1.0% in 2024, up from 0.1% in 2023, and further increasing to 1.7% in 2025 and 1.8% in 2026. However, this somewhat optimistic outlook could be disrupted by factors such as persistent inflation pressures or geopolitical shocks, which could slow down the expected rate-cutting cycle.

While this projection represents our best estimate, it does not account for potential changes in the international trading environment, and the path to economic normality is expected to be bumpy.

Quarterly real UK GDP, actuals and main scenario projections from Q2 2024.



Sources: PwC analysis, ONS.

02

Regulatory landscape

- UK regulatory agenda
- UK's corporate governance, audit and reporting regime
- FRS 102
- International tax and transfer pricing
- Regulator business plan update
- FCA's supervisory priorities for asset and wealth managers
- PRA's supervisory priorities for insurers

UK regulatory agenda

The UK is undergoing a period of significant FS regulatory reform, with the new government and regulators progressing a wide-ranging programme of repeal, review, and reform across the waterfront of FS regulation. Reform is expected to continue and embed over the course of several years, guided by political, economic and societal priorities. This slide intends to give a helicopter view of some of the key themes that are likely to be on labour's agenda over the next year, and as such things that IA functions should remain cognisant of as and when regulation evolves.

UK regulatory reform has been driven by key legislative and regulatory initiatives:

- **The Financial Services and Markets Act ('FSMA') 2023** establishes a new financial services regulatory architecture in the UK, entrenching overarching responsibilities with Parliament and His Majesty's Treasury ('HM Treasury') and delegating significant rule-making powers to the Financial Conduct Authority ('FCA') and Prudential Regulation Authority ('PRA').
- A broad package of further measures – the '**Edinburgh reforms**' – supplemental changes to the legislative framework and initiated an multi-year programme of regulatory and policy reforms.

UK authorities have made substantive progress on many of the reform initiatives over 2023-24 and will continue to consult and implement further changes in 2025. Details of the specific regulatory reforms and relevant timelines and milestones are provided in the rest of the pack.

The labour party has outlined its vision for a financial sector that aims to balance consumer protection, competitiveness, innovation and financial stability. It has identified six themes that will guide its focus on the sector, that will complement ongoing reforms undertaken through FSMA 2023 and the edinburgh reforms:

- **Inclusive growth**
- **International competitiveness**
- **Sustainable finance**
- **Innovation and fintech**
- **Consumer protection and financial inclusion**
- **Capital markets**

The King's speech, delivered on 17 July 2024, outlined the government's forthcoming legislative agenda and detailed further measures to advance policy and regulatory change in FS. This includes:

01 Bank resolution (recapitalisation) bill to enhance the UK's resolution regime by giving the BoE additional powers to respond to small bank resolution.

02 Pension schemes Bill to boost pension schemes' value to savers by introducing a range of measures including the consolidation of small deferred pension pots, introducing a value for money framework that will apply consistently across the pension market, and greater consolidation of the defined benefit pension market.

03 Draft equality (race and disability) Bill to introduce mandatory ethnicity and disability reporting for companies with 250+ employees.

The regulatory agenda is expected to develop and evolve over the course of the next parliamentary term. Policymakers and regulators will continue further initiatives focused on tailoring existing rules and regulation to better suit UK markets, whilst bolstering the competitiveness and growth of the UK's financial sector.

UK's corporate governance, audit and reporting regime

In January 2024, revisions to the UK Corporate Governance Code ('the Code') were published by the Financial Reporting Council ('FRC'). The Code sets a new bar for corporate governance and we expect its effects will be felt beyond those organisations who must comply as Boards will want greater transparency and assurance over risks and controls.

Who is impacted by these changes?

The listing rules require all premium listed entities to report against the Code.

Large private companies might also be impacted, but only to a limited extent, under the companies (Miscellaneous Reporting) regulations 2018 if they are required to disclose their corporate governance arrangements in their Directors' report and on their website, including information on whether they follow a formal governance code.

What is the proposed timeline?

All of the changes to the code are effective for financial periods beginning on or after 1 January 2025, with the exception of provision 29, which covers the new Directors' declaration over risk management and internal control described above. That is effective for financial periods beginning on or after 1 January 2026.

It is important to remember that until these effective dates, companies should follow the existing 2018 Code.

Key updates to the Code include:

- Annual controls declaration required – Boards will be required to make an annual declaration in the annual report on the effectiveness of all material controls as at the balance sheet date.
- Wide ranging scope covering all material controls – The declaration will cover all material controls, including (i) financial, (ii) operational, (iii) compliance controls and now also (iv) non-financial reporting controls.
- Basis of declaration to be disclosed – It will include a description of how the Board has monitored and reviewed the effectiveness of its risk management and internal control framework.
- Need to consider 'material' control deficiencies – It will also include a description of any material controls that have not operated effectively as at the balance sheet date, the action taken, or proposed, to improve them and any action taken to address previously reported issues.
- Incorporation of the 'Audit Committees and the External Audit: Minimum Standard' – Which covers audit committee responsibilities for the audit tender and monitoring the quality and effectiveness of the external audit has been included in the code so will apply on a comply or explain basis, from 1 January 2025, to all companies that apply the Code.
- Does not include withdrawn corporate reporting disclosures – Requirements for companies to have an audit and assurance policy and resilience statement on a comply or explain basis have not been included. Note that existing provisions relating to the viability statement are still in place.

UK's corporate governance, audit and reporting regime (continued)

Path to readiness for the new Code

For organisations who are new to the concept of a formal, broad-based controls and assurance framework, the path to readiness for the new Code will require a programme of work, supported by a cross-functional team and incorporates the following key stages.

Risk workshop

An initial workshop to determine how to adapt and use existing risk registers to support decisions around what's in scope and how to assess materiality.

Material controls workshop

Using existing risk and controls documentation to confirm a material control list to form the basis for the annual declaration. Controls can operate in any of the lines of defence, and may be preventative or detective. Some controls will be manual and others may be automated. Corresponding IT General Controls need also to be identified.

Identify gaps and prepare a remediation plan

Controls documentation will be needed to define the key controls in relation to material risks. Where controls are missing, do not adequately address the identified material risks or are not operating effectively, remediation plans should be developed and implemented.

Understand and assess current levels of assurance

Some of the new operational and non-financial disclosure controls that will be in scope for the annual controls declaration might already be tested and assured by second or third line teams from within the business or via third party specialists. Assurance maps provide a useful means of understanding the current assurance coverage. We recommend that the maps incorporate a thorough assessment of the quality of assurance as well as the quantity.

Testing

We recommend a phase of detailed testing before transition to self-assessment, in order to baseline the current status and apply a consistent approach. Many organisations are planning to test key controls one year ahead of the formal deadline for the controls declaration statement.

Transition to business as usual

The Code attestation applies from 1st Jan 2026 onwards.

UK's corporate governance, audit and reporting regime (continued)

Internal audit focus areas

The role of internal audit is to provide independent assurance that an organisation's risk management, governance and internal control processes are operating effectively and in compliance with regulations.

Key areas for internal audit to consider include:

- **Independent assessment** – Provide an independent and objective assessment of governance processes. Evaluate the effectiveness of the Board, Executive management, and internal controls to ensure they are aligned with best practices and regulatory requirements.
- **Internal control evaluation** – Check the process by which the Board reviews and evaluates the design and operating effectiveness of internal controls.
- **Readiness** – Help Boards conduct gap assessments against the new requirements to understand key areas where remediation is required to ensure compliance.
- **Ongoing assurance** – Developing an assurance map across the three lines of defence to assess the adequacy and effectiveness of the governance, risk and controls framework on an ongoing basis.

FRS 102

The FRC issued comprehensive improvements to financial reporting standards applicable in the UK and Republic of Ireland. The amendments are focused on updating UK's Generally Accepted Accounting Principles ('GAAP') accounting requirements to align more closely with the International Financial Reporting Standards ('IFRS').

The FRC has published 'Amendments to FRS 102 The Financial Reporting Standard applicable in the UK and Republic of Ireland and other FRSs – Periodic Review 2024' ('the Amendments') on 27 March 2024.

The amendments are focused on updating UK GAAP accounting requirements to align more closely with IFRS Accounting Standards in some areas, particularly with respect to revenue and leases, and making other incremental improvements and clarifications. The changes are significant and will require planning and preparation for companies to get ready in time. The changes are effective from 1 January 2026.

Overview of major changes

- **Revenue:** A single comprehensive five-step model is introduced for revenue recognition for all contracts with customers. An option to restate comparatives is included but is not mandatory. Application of the new revenue standard to complex revenue arrangements can cause changes to the current accounting treatment. Areas that can require effort and judgement include identification of performance obligations, principal versus agent considerations and variable consideration.
- **Leases:** The amendments remove the distinction between operating and finance leases for lessees, with more leases now recognised with an asset and liability on balance sheet. Restatement of comparatives is not required. The transition process will include the need to review of lease agreements, application of discount rates and calculation of lease asset and liability.
- **Other:** Various other incremental improvements and clarifications are designed to promote consistency with IFRS reporting including updated fair value measurement principles, revisions to the conceptual and pervasive principles, disclosures for supplier finance arrangements and updated guidance around share-based payments and accounting for uncertain tax positions.

Firms are recommended to perform an initial impact assessment to determine how accounting practices and the financial statements might be affected. This assessment will enable you to calculate the potential quantitative impacts on key areas in anticipation of the adoption date of 1 January 2026.

FRS 102 (continued)

Key considerations for firms

- Firms are required to implement the amendments from the accounting period beginning on or after 1 January 2026. New disclosures about supplier finance arrangements will be effective from 1 January 2025.
- Application of the new revenue standard to complex revenue arrangements can cause changes to the current accounting treatment. Areas that can require effort and judgement include identification of performance obligations, principal versus agent considerations, variable consideration etc.
- Lessees will be required to recognise lease assets and liabilities on the balance sheet. The process will include review of lease agreements, application of discount rates and calculation of lease asset and liability.
- The amendments to FRS 102 includes a number of simplifications and entities will need to assess the impact of simplifications including justification for application.
- There can be additional data requirements as a result of compliance with the accounting changes and related impact to systems and processes. This will require assessment as part of the implementation project.
- Quantification of changes can have an impact on financial metrics and covenants. Firms can perform financial modelling to assess impact and form response.
- Companies will be required to apply the transition requirements and calculate the impact of the accounting changes on opening balance sheet. This can have a significant impact and will require the appropriate focus.

Internal audit focus areas

- Evaluate the ongoing preparations for the FRS 102 amendments. This encompasses reviewing the robustness of governance and oversight frameworks, creating a project plan to ensure timely and effective updates to policies, processes, and systems.
- Assess the proposed approach to implement the changes required, including short-term manual approaches versus more comprehensive strategic solutions if they are required.

International tax and transfer pricing

What's on the risk agenda?

International taxation continues to undergo significant change. As part of the Organisation for Economic Cooperation and Development (OECD's) efforts to counter tax avoidance by the largest multinational groups and fuelled by economic pressure on governments to maintain or increase tax revenues, new public country by country reporting **(CbCR) and global minimum effective tax rate (ETR) regimes** are now starting to come into force in many countries, including the UK.

The new regimes aim to increase transparency over taxpayers' affairs for tax administrations and to ensure a fairer allocation of profits and taxes between jurisdictions, including developing economies. These rapid changes are creating complexity and uncertainty for businesses, placing increased pressure on resources, and pose potential reputational risks for effected enterprises.

What's changing?

01

Transfer pricing

In the UK, the Transfer Pricing Records Regulations 2023 introduced a new requirement for large multinational businesses to prepare and maintain transfer pricing documentation in a set manner - the OECD master and local file format - an approach already enacted by many other countries.

This new UK transfer pricing documentation requirement is effective for accounting periods beginning on or after 1 April 2023 for groups with consolidated global revenues above €750M. Groups below this threshold are strongly encouraged by HMRC to prepare documentation in the same format.

It is particularly important to consider the following when assessing a UK taxpayer's TP documentation under the new rules:

i. The right for HMRC to request transfer pricing documents outside of a transfer pricing enquiry.
ii. The removal of the requirement for documents to be in the "power and possession" of a UK entity when they are in the "power or possession" of another group entity. and
iii. A presumption of carelessness where a taxpayer fails to do the work necessary to maintain or to produce relevant records on request, with associated implications for penalties (of up to 100%).

02

Country by country reporting ("CbCR")

CbCR was first introduced in 2016, is now becoming public, meaning that annual data on the operations, revenues, profits, taxes and headcount of large multinationals by country will increasingly be accessible to the press and the public.

Under an OECD Inclusive Framework, more than 140 countries have now agreed to enact a two-pillar solution to address the challenges arising from the digitalisation of the economy, although implementation timetables differ between countries, increasing complexity for taxpayers.

03

Pillar Two

It is a once in a generation tax event for organisations, which introduces a global minimum ETR of 15% for the largest multinational groups.

EU member states unanimously adopted a directive which required them to introduce the rules from 31 December 2023. Many other countries are also working on their domestic rules to implement Pillar Two.

UK legislation has been enacted which introduces the OECD's Pillar Two model Income Inclusion Rule into UK law, as well as a domestic top-up tax. These rules first apply to accounting periods commencing on or after 31 December 2023. In addition, the UK is expected to introduce an Undertaxed Profits Rule with effect from 2025.

Whilst the UK has addressed some of the issues and complexities raised in respect of the OECD model rules, a number still remain.

Only groups with qualifying, that is, high quality and accurate CbCR reports prepared on a set basis, will be able to access the Pillar Two transitional safe harbour provisions, which in effect permit the use of that qualifying CbCR data to calculate and report Pillar Two tax liabilities, simplifying the compliance and reporting process significantly.

Groups with non-qualifying CbCR data will have to undertake substantially more work to satisfy the new multi-jurisdictional compliance requirements, which could be both time-consuming and costly.

International tax and transfer pricing (continued)

Key considerations for firms

- A Pillar Two readiness and compliance plan is essential to avoid the risk of being noncompliant in key jurisdictions.
- Strong transfer pricing controls are an important factor in easing the Pillar Two transition since late, i.e. post-closing transfer pricing adjustments cannot be reflected in the CbCR anymore. Making any adjustments to the post-close financial statement figures used for the CbCR, will disqualify it for the Pillar Two transitional regime.
- Last minute / late fixes could be disruptive and expensive, therefore getting ahead of this challenge is much more efficient and less costly.
- There is a need to generate new data points from multiple sources as compared to current needs today. Assessing and remediating gaps is necessary before the first deadline.
- Pillar Two may impact a multinational group's effective tax rate and it will be important to understand the magnitude of that impact early to avoid surprises.

Internal audit focus areas

- Assess how firm’s have approached the new tax changes from a governance and project management perspective.
- Assess the firm’s approach to generating the new data points, and remediating gaps that have been identified.
- Assess the firm’s approach to upskilling staff / senior management to be able to meet the new requirements.
- Assess the capabilities and resources of the tax function to maintain data, processes and controls, to keep abreast of developments, track compliance and to communicate effectively with internal stakeholders and tax authorities.
- Assess what controls are currently in place over these tax areas, and how might they be improved to make the process more efficient and reliable.

Regulator business plan update

The Financial Conduct Authority ('FCA') and Prudential Regulation Authority ('PRA') have set out their priorities for the year ahead, and the following provides key updates in the respective business plans.

The FCA

The FCA issued its Business Plan 2024/25 on 19 March 2024, detailing its priorities and plans for the year ahead. The business plan sets out how the FCA will deliver on its strategy, as it enters the final year of its three-year strategy (2022-2025). The strategy is based on three themes and it is underpinned by 13 commitments.

Acknowledging the breadth of change enabled by the Edinburgh eforms, and ongoing work to repeal EU law under the Smarter Regulatory Framework, there are limited new initiatives.

For 2024/25, the FCA plans to focus on three priority commitments, and they are:

01 Putting consumers' needs first.

02 Reducing and preventing financial crime.

03 Strengthening the UK's position in global wholesale markets.

Consumer needs - The FCA will continue its extensive supervisory work to test firms' implementation of the consumer duty and drive better consumer outcomes, through multi-firm work and market studies.

Wholesale markets - The FCA will continue to progress work implementing the outcomes of the wholesale markets review and Edinburgh reforms.

This has so far included completing reforms to the listing regime, publishing proposals for the new public offer and admission to trading regime, and confirming changes to rules on paying for investment research. The FCA also plans to finalise revised frameworks for commodity derivatives and non-equity transparency, implement the consolidated tape ('CT') for bonds, and decide on the approach for an equities tape.

Other areas of focus include supporting industry work on T+1 settlement changes and tokenisation, and working with His Majesty's Treasury ('HM Treasury') on launching the Private Intermittent Securities and Capital Exchange System ('PISCES') platform and digital securities sandbox.

The FCA also highlights work to improve its responsiveness to episodes of heightened market volatility, and to tackle market abuse, particularly in the fixed income and commodity markets.

Financial crime - The FCA will continue to proactively assess the anti money laundering systems and controls of those firms deemed higher risk, and to strengthen its supervision of firms' sanctions systems and controls.

The FCA also plans to increase investment in its systems this year, to further its data-led approach to target higher-risk firms and activities. It says it will expand its analytics and intelligence-gathering capabilities to better spot and track potentially fraudulent activity.

In addition to the three priorities covered above, we would also Particularly draw firms' attention to work planned under the following two commitments:

Shaping digital markets to achieve good outcomes - The FCA is continuing to assess the impact of Artificial Intelligence ('AI') on UK markets to better understand the risks and benefits, re-affirming its 'pro-innovation and technology-agnostic approach'.

The regulator adds that it will continue to robustly investigate digital consumer journeys and firms using sludge practices.

Improving the redress framework - The FCA highlights plans to consult later this year on guidance for how firms deal with redress, and on complaints reporting. It also plans to publish a response to the Advice Guidance Boundary Review ('AGBR') discussion paper in the next 12 months, and has set aside £1.9m for this work.

Regulator business plan update (continued)

Prudential Regulation Authority (PRA)

The PRA published its Business Plan 2024/25 on 11 April 2024, setting out its strategic priorities for the year:

- Maintaining the safety and soundness, and continued resilience of the banking and insurance sectors.
- Identifying new and emerging risks, and developing international policy.
- Supporting competitive and dynamic markets, alongside facilitating international competitiveness and growth.
- Running an inclusive, efficient and modern regulator within the central bank.

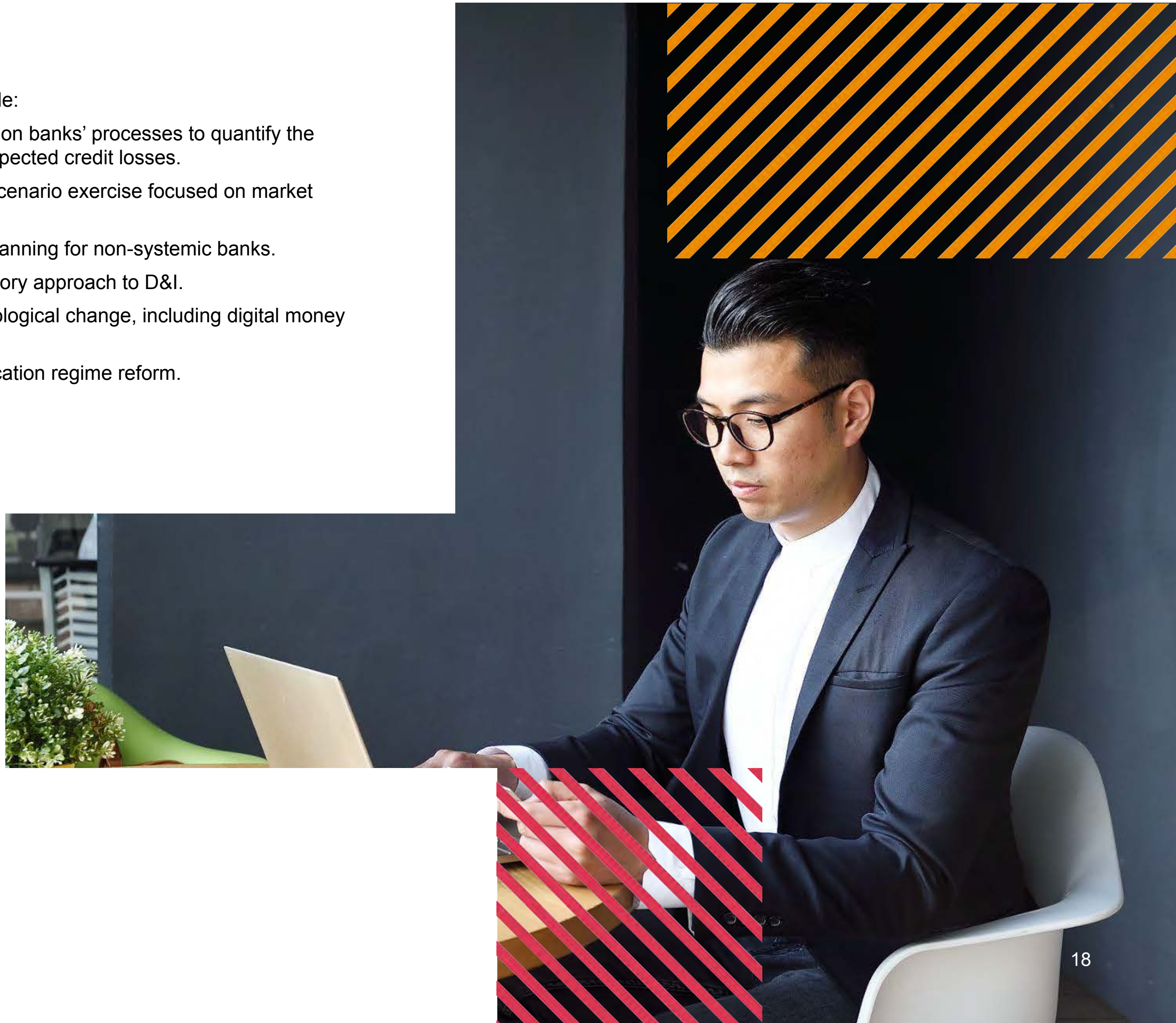
The business plan provides an overview and update on a number of ongoing priorities, including: Basel 3.1 implementation, the Strong and Simple framework, ring-fencing reform, risk management, operational risk and resilience, climate risk, FSMA 2023, and diversity and inclusion (‘D&I’).

In 2024, the PRA continues to build on the existing themes and priorities:

- Assess firms’ embedding of the model risk management (‘MRM’) expectations in supervisory statement (‘SS’) 1/23 and evaluate the impact of AI on model risk.
- Consult on ring-fencing regime changes after a cost-benefit review and continue providing HM Treasury with technical advice to refine legislation and evaluate long-term reform feedback.
- Take on direct oversight of Critical Third Parties (‘CTP’), aiming for full implementation of the critical third-party regime in 2025.
- Monitor and assess firms’ abilities to manage cyber threats and engage with firms on their execution of large and complex IT change programmes.

Other emerging priorities include:

- Publishing thematic findings on banks’ processes to quantify the impact of climate risks on expected credit losses.
- A system-wide exploratory scenario exercise focused on market stress.
- New policy on solvent exit planning for non-systemic banks.
- A consultation on the regulatory approach to D&I.
- The implications from technological change, including digital money and banks’ use of AI.
- Senior managers and certification regime reform.



FCA’s supervisory priorities for asset and wealth managers

See below for an overview for FCA’s supervisory priorities for asset and wealth managers and page references for where further details are provided.

Product governance

ESG and sustainable investing

Page 89

ICARA and wind-down plans

Page 36

Product liquidity management

Operations and resilience

Financial resilience

Adviser charges

Interest on cash balances

Consumer duty

Page 25

Retirement income advice

Vulnerable customers

Complaints

03

Hot spots

Contents

Conduct and governance

People and organisational culture

What's on the risk agenda?

Culture is now being recognised by CEOs as a powerful strategic differentiator. Successfully aligning culture and ways of working to strategic goals can bring a competitive edge through increased engagement, productivity and staff retention. Conversely getting culture 'wrong' can have significant regulatory, financial and reputational impacts.

Regulators are also focussed on culture and behaviours – particularly on leadership messages and psychological safety, which are critical to underpin compliance and ensure that organisations focus on what is right for customers, workers and wider stakeholders. There is also increased focus on risk culture; how behaviours such as accountability along with leadership and the work environment influence risk management and decision making.

Firms not only need to demonstrate a strong tone from the top but also that they have set people up for success in management roles across the organisation. As such a focus on relevant communications, training, ways of working, as well as reward and consequence management are key to drive the desired culture and behaviours.

Internal audit is uniquely positioned to offer an independent and robust assessment of 'people risks'. Successful assurance requires a diligent and focussed approach, with tailored recommendations to address root causes, and strong engagement and collaboration with senior leaders to ensure change is enacted.

Across this page and the next, we outline four trends for 2024 and beyond which are influencing the nature and relative extent of 'people risks' facing businesses today. We then outline the key components of the control environment relevant to these risks which are ripe for internal audit focus.

> A sound workforce strategy is one that connects transformation ambitions with exceptional workforce planning, and provides workers with the reassurance they'll be equipped with the skills and tools they need to thrive'
>
> **PwC Hopes and Fears Survey 2024***

What's changing?

We know from our latest Hopes and Fears Survey 2024* the adoption of new technology, the pace of business transformation, the focus on new skills and the imperative for workplaces to be inclusive, fostering equality and embracing diversity – are all changing the profile of 'people' risks from the perspective of employees as well as CEOs.

1. Workforces will be transformed by the AI revolution - organisations can either meet these challenges head on or risk large scale disruption

Advances in technology will fundamentally change the way we work, with workforce requirements and the business thinking radically changing in the coming years. Based on the PwC 2024 AI Jobs Barometer, the need for AI specialist skills is rising, with the number of AI jobs postings increasing 7x since 2012, outpacing growth in all job postings by 3.5x. Roles with AI specialist skills also command a significant wage premium, with an average wage premium of 14% for job vacancies which require AI skills in the UK.

AI is also playing a growing role in deciding who enters and succeeds in the workforce; already we have seen widespread adoption of AI in recruitment process, and further integration is expected across the entire talent management lifecycle.

AI will increase worker efficiency, change skills requirements and contribute to the pipeline of future leaders; leading organisations are proactively considering these impacts and leveraging the resulting changes to purposefully transform their workforce and explore new market opportunities. Conversely, organisations that do not take a proactive approach may find that their workforce becomes ill equipped or unable to meet future strategic objectives.

2. The skillset of the future employee will be vastly different to today

Skills needs are changing rapidly, resulting in the need for continual upskilling to meet evolving requirements. Already organisations are struggling with acute talent shortages in key roles, with 78% of business leaders reporting some extent of skills shortage within their organisation – 68% in relation to technology, per our survey*.

As repetitive tasks become the domain of technology and humans take on more creative and innovative roles, leadership behaviours will become a key competency of successful future employees. Given the economic outlook and need for productivity, culture will be integral to fostering high performance teams and organisations.

Given competition in the talent market and the pace of change, organisations must proactively identify future skills requirements and begin to upskill their workforce to meet these needs.

* See linked here | **PwC Hopes and Fears Survey 2024**

People and organisational culture (continued)

3. Business transformation and change continues but a gap widens on understanding the ‘why’

Organisations face a range of pressures brought on by the need to balance transformation and creating value; with compliance, changing regulations, a fast-moving and unpredictable risk landscape, and growing competition.

Our survey* results show that employees are feeling the impact of change, with two thirds reporting that they have experienced increasing levels of change at work in the previous 12 months, however 40% don’t understand why change needs to happen. Leading organisations create trust and engagement and protect against change fatigue and burnout through:

- Fostering a culture that is agile and adaptable to change.
- Openly engaging employees in discussions around uncertainty in the political and/or economic environment and its impacts on the business.
- Creating a strong change narrative which leaders are aligned around to deliver a consistent message to their people.

4. Transparency requirements will become more demanding

New and anticipated regulatory requirements are increasing demands for transparency on workforce diversity and pay equity, with global organisations facing an increasingly complex regulatory landscape (we have further outlined some of the DE&I requirements on page 100). In the future, organisations should be ready to report more detailed and broader information on their DE&I strategy and outcomes.

Against this backdrop, many organisations are making voluntary disclosures beyond the legal requirements and increasing transparency around pay and diversity which requires sound data and thoughtful narrative. Organisations need to ensure they have the capability to meet evolving requirements, and should consider how they will communicate broader messaging regarding disclosures both internally and externally.

* See linked here | **PwC Hopes and Fears Survey 2024**

Internal audit focus areas

In the light of cultural and people changes outlined, internal audit should focus on the following key areas:

Culture and behaviours

- Evaluate the firm’s cultural proposition ensuring a clear set of values and behaviours have been defined, and review mechanisms in place to embed these. Consider the alignment of the values and behaviours to the strategic objectives of the organisation.
- Evaluate leadership competencies and development opportunities across the organisation (paying attention to leaders at all levels, not only senior leadership), ensuring leaders have the skills and tools to foster a high performing and inclusive culture.
- Assess processes and capability to managing workplace conflicts and whistleblowing, and / or conduct investigations into widespread and/or systemic culture issues to identify remedial action.
- Evaluate the effectiveness of reinforcers to promote and reward desired behaviours, for instance, including but not limited to: ethical frameworks, codes of conduct, training programs, performance management systems, and recognitions schemes (both formal bonuses and informal recognition mechanisms).

Workforce planning

- Evaluate the skills, capabilities and workforce needs aligned to the delivery of the business strategy; Consider productivity, location analysis, sourcing strategies, employee value proposition and reskill/upskilling.

Diversity, equity and inclusion (‘DE&I’)

- Evaluate the DE&I Strategy, ensuring consideration has been given to relevant qualitative and quantitative DE&I data, internal and external forces and the broader business and people agendas, and / or assess progress against the same.
- Evaluate the design and effectiveness of the DE&I operating model and programme and / or specific initiatives, including whether talent management processes enable inclusive and equitable outcomes.

Employee Value Proposition (‘EVP’) and talent management

- Evaluate the workforce/people strategy and EVP, ensuring it appropriately considers and addresses evolving workforce trends and is aligned to and supports the achievement of the business strategy and / or assess progress against the same.
- Evaluate the approach to workforce wellbeing, assessing steps taken to support employee wellbeing and cultivate a positive work environment.
- Review talent management lifecycle processes such as recruitment, training and development, performance management and succession planning to ensure effective design and operation.

Governance and accountability

- Review governance and accountability frameworks for managing people risks, ensuring appropriate oversight and leadership and assessing decision making capabilities.

Consumer duty

The consumer duty ('the Duty') has been effective for open products and services since July 2023, and has applied to closed products and services since July 2024. It introduces a more outcomes-focused approach to consumer protection and sets higher expectations for the standard of care that firms should provide to their customers.

The Duty introduces a new consumer principle which requires firms to deliver good outcomes for retail customers. The four outcomes that underpin this principles are: (1) the governance of products and services, (2) fair price and value, (3) consumer understanding and (4) consumer support.

When supervising and enforcing against the Duty, the FCA makes it clear that it will focus on the issues which present the greatest risk of consumer harm. The FCA's focus and response will be governed by data and metrics, to ensure it responds proportionately to any harm identified. A summary of some of the FCA's expectations under the Duty are set out below:

- **Business led:** Acting to deliver good outcomes should be at the heart of firms' strategies and business objectives. The Board will take full responsibility for ensuring the Duty is properly embedded within the firm. The FCA is looking for evidence that the Duty has been considered at every level.
- **Monitor outcomes not compliance:** Data and other insights should evidence outcomes for consumers at all stages of the customer journey. The FCA is looking for firms to adopt a 'predict and prevent' approach to outcomes. The FCA expects firms to ensure they have comprehensive approaches for monitoring outcomes for different groups of customers, including those with characteristics of vulnerability.
- **Communicate and engage:** Customers need clear information that they can understand, as well as access to effective support that can enable them to make informed decisions and pursue their financial objectives.
- **Identify risk of harm:** Products, processes and services should be analysed to understand the potential for consumer harm. Data should be used to identify whether harm has actually arisen. Firms should take appropriate action to mitigate the risk of actual or foreseeable harm.
- **New products and services:** Innovation should be driven by the needs of a firm's target market, at a value point that is fair and where good outcomes can be monitored.
- **Existing products and services:** Product design, services standards, and consumer access to support will need to be continuously monitored to ensure they meet the needs, characteristics and objectives of the target market. The FCA wants to be consulted if a firm seeks to close old products.

The FCA issued portfolio letters to asset managers in February 2023 and May 2024, and to wealth managers in November 2023. The letters outline the sector-specific themes and risks the regulator has identified as firms implement the Duty for open and closed products and services. The FCA highlighted a set of priority areas for asset and wealth management ('AWM') firms to consider, including the assessment of fair value and the identification and treatment of customers with vulnerable characteristics.

Consumer duty (continued)

Key considerations for firms

The FCA has outlined its expectations across the Duty's four outcomes as below:

- **Consumer understanding:** Firms to go beyond communicating in a way which is clear, fair and not misleading – and take steps to ensure communications are 'reasonably likely to be understood', and consider how their overall approach to communicating can equip consumers to make decisions in their interests.
- **Products and services:** Meeting the needs, characteristics and objectives of their customers, and allowing customers to act in their interests, should be central to how firms design and distribute products/services. Firms should take reasonable steps to ensure products/services are distributed to the intended market, and review the fairness of contract terms.
- **Consumer support:** Post-sale interactions should be as simple and accessible as the sales processes and free of unreasonable barriers which could prevent customers from acting in their interests. Firms should be alert to customers' evolving support needs and should have sufficient capacity to support customers via various channels.
- **Price and value:** Firms should assess whether all products/services deliver fair value (meaning its benefits are reasonable relative to its price), on an initial and ongoing basis. Poor value products/services should be dropped or altered before they come to market. The Duty aligns with existing assessment of value rules applicable to parts of the sector. Firms should continue to meet expectations set by these rules, particularly where the FCA has raised concerns, for example, in relation to fee/charges disclosures.

Internal audit focus areas

- Review and assess the effectiveness of the implementation of the changes made by firms to comply with the Duty, ensuring firms align with the regulators' expectations, in particular addressing the sector-specific points raised by the FCA.
- Review and monitoring of how firms are delivering good customer outcomes, how they are identifying foreseeable harm and the steps taken to mitigate this risk.
- Review of the quality and granularity of data that firms are using under each of its products/services and the Duty outcomes. This should validate the firm's ability to effectively monitor the outcomes customers are receiving, including for different customer cohorts, and identify the risk of consumer harm.
- Review of the governance and oversight processes, ensuring outcomes monitoring data is presented to Boards and executive committees with appropriate analysis and narrative, and that targets and tolerances are subject to sufficient scrutiny.

Wholesale markets reforms

His Majesty's Treasury ('HM Treasury') and the regulators are developing a wide-ranging set of reforms to wholesale financial market rules, reflecting market developments as well as the UK's post-Brexit regulatory agenda.

Many of the wholesale market reforms - covering primary and secondary markets as well as post-trade - take forward the recommendations of the Government's Wholesale markets review, Edinburgh Reforms and Mansion House announcements, and form part of the multi-year programme to repeal and replace retained EU law. The FSMA 2023 and a range of statutory instruments implement various elements, while others are still in development.

Primary markets

- **Listings reforms:** Following the Lord Hill listings review, the FCA has implemented various changes to the listing regime. The FCA finalised rules that overhaul the listings rules for equities in July 2024.
- **Public offers and admission to trading regime:** HM Treasury is legislating to replace the Prospectus Regime with a new Public Offers and Admission to Trading Regime ('POATR').
- The FCA consulted in July 2024 on the new requirements for issuers under the POATR. This includes a proposal for offers of securities above a certain threshold to be made public through a public offer platform. Operating a public offer platform will be a new regulated activity.

Secondary markets

- **Equity markets:** In April 2024, the remaining elements of the FCA's reforms to equity secondary markets, as set out in PS 23/4, went live. Changes were made in areas that were not contingent on legislative change and could be introduced via amendments to existing FCA rules and guidance e.g., removal of the double volume cap and share trading obligation.
- **PISCES:** HM Treasury is prioritising proposals to introduce a new Private Intermittent Securities and Capital Exchange System ('PISCES'). PISCES is intended to provide an intermediate step to public capital markets for private companies or PLCs looking to scale up. The regulatory framework for PISCES will be tested and developed through the Financial Market Infrastructure ('FMI') Sandbox.
- **Commodity derivatives:** FSMA 2023 transfers the setting of position limits from the FCA to trading venues. The FCA has consulted a range of other changes, covering the regimes for position limits, position management controls, position reporting and position exemptions. Planned reforms to the ancillary activities test have been paused following industry feedback.
- **Securitisation:** A new legislative framework has been created that allows the regulators to make rules in relation to securitisation. The FCA and PRA have published new firm-facing rules that will come into effect from 1 November 2024, subject to repeal of the UK Securitisation Regulation ('UK SR'). A further consultation on reporting and disclosure requirements, and the definition of private and public securitisations, is expected later in 2024.
- **Short selling:** The threshold for reporting net short positions was increased to 0.2% in February 2024 via an Statutory Instrument ('SI'). HM Treasury has also published a draft SI that would create a new regulatory framework for short selling and provide the FCA with a range of rule-making powers. The FCA will consult on detailed aspects of the new regime for short selling in due course.

Wholesale markets reforms (continued)

HM Treasury and the regulators are developing a wide-ranging set of reforms to wholesale financial market rules, reflecting market developments as well as the UK's post-Brexit regulatory agenda.

Post trade

- **T+1 settlement:** Authorities in the UK, EU and Switzerland are considering the implications of shortening the securities settlement cycle from T+2 to T+1. T+1 settlement will require firms to adopt a series of technological and operational changes, and represents a major change programme affecting a wide range of market participants. It also presents opportunities for firms to realise efficiency gains, automate processes and reduce costs.
- The UK has committed to adopting T+1 no later than 31 December 2027. Consultation proposals from the UK technical group on T+1 are expected in September 2024, and are likely to include recommendations on whether the UK's adoption of T+1 should align with the EU and Switzerland.
- **UK European Market Infrastructure Regulation ('EMIR'):** Changes to the derivatives reporting framework under UK EMIR go live at the end of September 2024. The BoE has stated that it will work with HM Treasury to prioritise replacing EMIR with UK-specific rules but without a lowering of standards.
- **Designated reporter regime:** The FCA has introduced a new Designated Reporter regime, that establishes which party to a transaction has the obligation to publicly report.
- **UK Markets in Financial Instruments Regulation** ('**MiFIR'):** The FCA has committed to a review of UK MiFIR transaction reporting, and will consult on post trade risk reduction later in 2024.

Wholesale data

- **Consolidated tape:** The FCA has issued final rules on the framework for a bond consolidated tape, and is expected to publish a further update on an equities consolidated tape ('CT') later in 2024. The bond CT Provider is expected to be appointed and become operational in 2025.
- In March 2024, the FCA confirmed it would proceed with its original proposals to not require the CT provider to make payments to data providers. However, the FCA has committed to reviewing this position following the first five-year CT Provider contract period.
- **Wholesale Data Market Study:** The FCA has published the findings of its Wholesale Data Market Study that focused on competition dynamics in the markets for benchmarks, credit ratings data, and market data vendors. The FCA identified a number of common competition themes across all three markets but ruled out making a referral to the Competition and Markets Authority. Instead, the findings will inform ongoing and planned reviews into aspects of the regulatory framework.
- **Reasonable commercial basis framework:** The FCA has committed to exploring potential changes to the 'reasonable commercial basis' framework under UK Markets in Financial Instruments Directive ('MIFID'), to address concerns about the complexity of licensing practices employed by data generators. This review will commence once the impact of the introduction of consolidated tapes can be assessed.
- **Payment for investment research:** The FCA has finalised changes introducing an additional option for the payment of investment research, following a review that found the current rules to be operationally complex and potentially advantageous to larger firms. The additional option would permit 'bundled' payments provided certain requirements are met.

Market transparency

- **Fixed income and derivatives transparency regime:** HM Treasury's Wholesale Markets Review proposed changes to the transparency regime for bonds and derivatives, to improve transparency and remove inappropriate instruments from scope of the regime.
- The FCA has consulted on proposals that would make changes to the scope of instruments subject to transparency requirements, to pre- and post-trade reporting transparency obligations, and to the definition of when a firm must register as a Systematic Internaliser. The FCA is expected to confirm its final rules later in 2024.
- **UK Benchmarks Regulation (BMR):** HM Treasury has committed to implementing potential changes to ensure the UK has an appropriate regime for third country benchmarks, and has extended to current regime's transitional period until the end of 2030 to provide sufficient time for this review. HM Treasury will also undertake a more holistic review of the UK BMR, including taking into account the findings from the FCA's wholesale data market study.

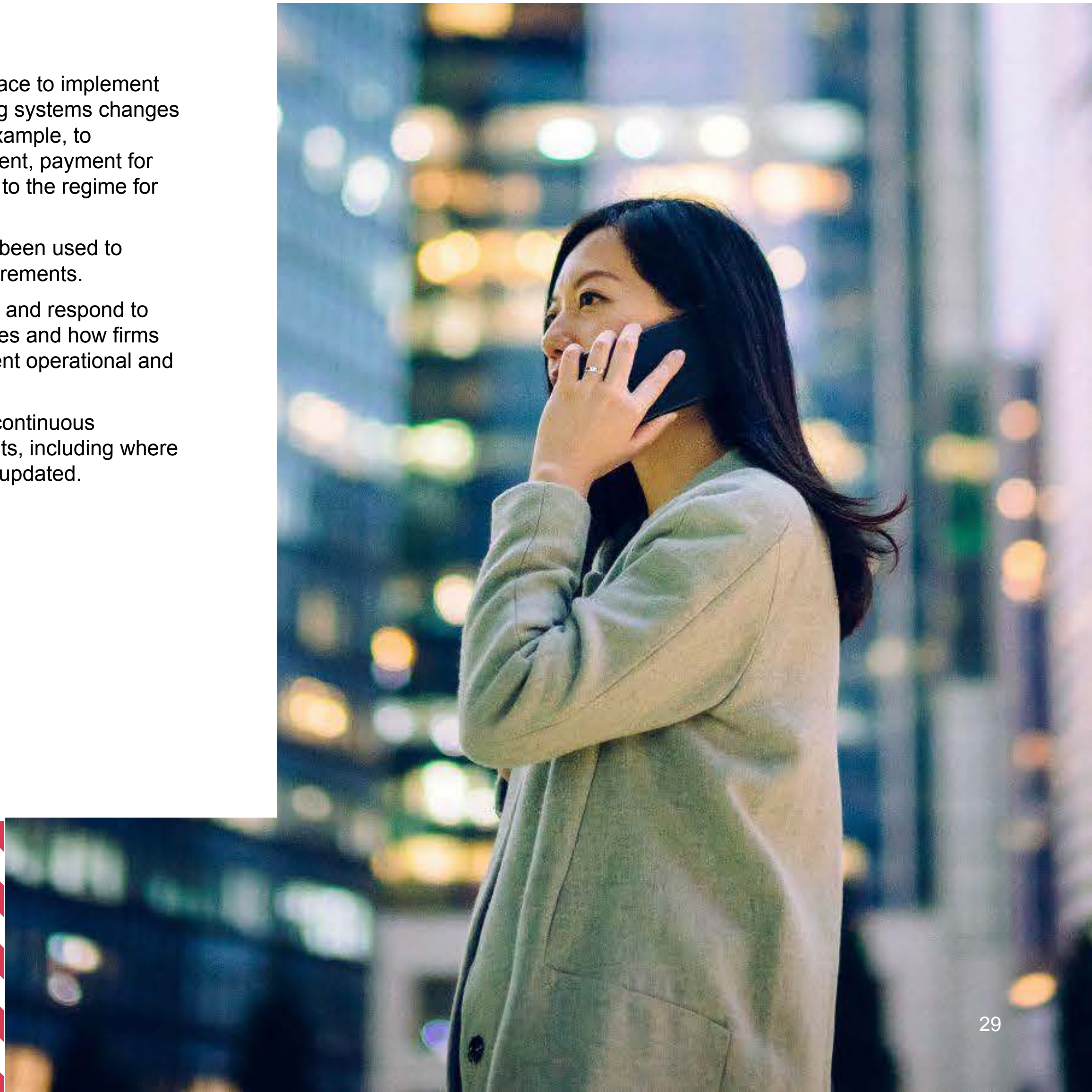
Wholesale markets reforms (continued)

Key considerations for firms

- The Government and FCA have stated that reforms to the wholesale markets regulatory framework are focused on maintaining high standards whilst reducing and removing unnecessary or complex regulatory burdens, and supporting innovation in the market.
- In particular, UK authorities are aiming for the changes to bring about improvement in transparency and market efficiency by enabling better identification of price-forming transactions and improving the consolidation of trade reports from multiple sources. Tailoring regulation to suit UK markets, and providing for greater proportionality, are other aims of the various reform elements.
- Many updates needed are technical and it will take firms time to review them, as such firms should consider the impact on their business and what needs to change. In some cases, this may require investment in operational processes, reporting systems and compliance procedures.
- Firms should also be alert to the different approaches taken by the UK and EU to the regulation of wholesale markets, post-Brexit. Given the cross-border nature of wholesale activity, firms will have to deal with the operational complexities of divergent rules.

Internal audit focus areas

- Assess and review the processes in place to implement operational, technological and reporting systems changes to reflect the regulatory reforms. For example, to post-trade transparency, faster settlement, payment for investment research, and the changes to the regime for commodity derivatives.
- Review how systems functionality has been used to demonstrate compliance with the requirements.
- Assess the controls in place to monitor and respond to divergence between UK and EU regimes and how firms are prepared to manage any subsequent operational and compliance complexities.
- Review of the processes for ensuring continuous compliance with regulatory requirements, including where expectations or obligations have been updated.



Overseas funds regime

The overseas funds regimes provides access to the UK for EU-domiciled undertakings for the Collective Investment in Transferable Securities ('UCITS') (excluding money-market funds ('MMFs')). Those funds operating under the legacy temporary marketing permissions regime must apply in a given 'landing slot' in order to continue to market to UK clients. Landing slots are being allocated by the FCA and will run from October 2024 to July 2026.

Following the UK's departure from the EU, existing Undertakings for the Collective Investment in Transferable Securities ('UCITS') funds were able to continue to market into the UK under the Temporary Marketing Permissions Regime ('TMPR'). New funds could not launch, nor take advantage of this, and instead had to utilise s.272 provisions, which are resource intensive.

HM Treasury and the FCA set out a roadmap for the Overseas Funds Regime ('OFR') on 1 May 2024. Prior to this, the UK Government had to deem the EU-UCITS regime (excluding MMFs) equivalent to UK fund rules, which allowed the FCA to facilitate permanent market access, subject to legislation.

In the run up to the new regime, the TMPR, subject to legislation, is being extended until the end of 2026, to allow smooth transition to the new OFR.

Existing funds under the TMPR will be allocated a three-month 'landing slot' (based on alphabetical order of the manager) to apply to be recognised under the OFR. Any operator missing their slot will lose permission to market in the UK. New funds will also be able to launch via the OFR.

The FCA confirmed the final rules on 17 July 2024. This included detail on the data and information needed, when the new online system is available.

The OFR is expected to be open for new funds (not already taking advantage of the TMPR) from September 2024, with the 20 slots for existing funds to apply commencing monthly from October 2024, and the final slot commencing in July 2026. A manager beginning with an early letter in the alphabet will need to submit in a three month window commencing in October, November or December 2024. Failure to meet this deadline would automatically see a fund fall from the TMPR and not permitted to be marketed to UK retail investors.

Overseas funds regime (continued)

Key considerations for firms

- For any firms that have taken advantage of of the TMPR, they must also make use of the relevant ‘landing slot’, failure to do would lead to the fund being removed from the TMPR and banned from promotion to retail investors.
- The FCA has two months to make a decision on whether to recognise the scheme.
- The data requirements are not necessarily onerous in their own right, but submission must be made on time and correct the first time. Firms with multiple funds will need to manage this for all funds during the same landing period.

Internal audit focus areas

- Understand and assess management’s progress on transition to OFR, including decisions made and preparedness for the upcoming three month ‘landing slot’.
- The FCA makes very clear that only completed applications will be accepted, firms must ensure they provide all relevant information. Internal audit should review the completeness of the information management has provided.

Oversight of appointed representatives

An Appointed Representative ('AR') can perform regulated activity under the responsibility of an authorised firm. In September 2024 the FCA published findings of its review into how principal firms are embedding the new rules it introduced in 2022 to enhance its AR regime. The new regime aims to further protect consumers and address harm in the sectors within which principal firms and ARs operate. In its review the FCA found that principal firms had made some effort to comply with its new rules, however there was room for improvement in areas such as self-assessments and annual reviews.

The AR regime allows firms to offer certain financial services activities without having to be directly authorised. An AR carries on regulated activity under the responsibility of the authorised 'principal' firm. When a principal appoints an AR, it takes on responsibility for the regulated activities carried out by the AR. More specifically, the principal is responsible for making sure the AR is fit and proper, complies with the FCA's rules, and operates within the scope of their appointment.

New FCA expectations

Further to its proposals, the FCA strengthened the AR regime through PS22/11, which came into effect in December 2022. Principals must now provide more information to the FCA on their ARs, including how they are overseen. Principals are required to:

- Enhance oversight of their ARs, ensuring they have adequate systems, control and resources.
- Review and monitor the risks their ARs present to customers and markets in the same way they would do for their own business.
- Review information annually on their ARs' activities, business and senior management (being clear on when an AR relationship should be terminated).
- Notify the FCA of new AR relationships, 30 calendar days before they take effect.
- Provide the FCA with annual complaints and revenue data on each AR.

An FCA priority

Improving the AR regime is a key FCA priority. The FCA found principles and ARs have greater levels of complaints and supervisory cases than directly authorised firms – indicating wide-ranging harm. When the FCA launched a consultation in December 2021 to address some of the harms it identified (culminating in the enhanced AR regime), the Government also launched a call for evidence.

The Government considered that more evidence is required before it can decide whether legislative reform is necessary in relation to the AR regime. Therefore the aim of the call for evidence was to gather industry views on how the AR regime is used and how effectively the regime works in practice.

The FCA recently published findings of its review into how principal firms are embedding its new rules on effective AR oversight. It set out a series of good practice and the areas of improvement it identified. Principal firms should ensure they are completing adequate self-assessments and annual reviews, and ensure that AR onboarding and termination procedures are robust and in line with the new rules.

Consumer Duty implications

The FCA confirmed when making changes to its AR regime that:

- The Consumer Duty goes hand-in-hand with some of the changes it made to the AR regime.
- Principal firms must ensure that their ARs comply with the Consumer Duty.

Oversight of appointed representatives (continued)

Key considerations for firms

Overall, the FCA expects consumer confidence to increase due to the improved outcomes from dealings with principals and ARs. Maintaining a range of effectively operating principles and ARs across sectors will also better enable a wide selection of products and services to be available to consumers. Under the enhanced AR regime, principal firms should ensure they:

- Understand their responsibilities in relation to ARs and have robust oversight of their ARs. This should include ensuring there is robust governance in place to enable principals to take more effective responsibility for their ARs.
- Have clear systems and controls in place to allow them to take a proactive approach in addressing problems with ARs that have the potential to, or already do, cause harm to consumers/markets.
- Have adequate processes and systems in place so that data is reported to the FCA in a timely manner. For example, processes must drive the principal to notify the FCA of a future AR appointment 30 calendar days before the appointment takes effect.

Internal audit focus areas

- Ensure that principal and AR roles, responsibilities, and expectations are clearly defined in written agreements. Review processes and procedures to ensure the obligations within the agreements are being adhered to by both parties.
- Assess the quality of the information received from ARs, ensuring this enables the principal to effectively understand AR activities, business and senior management.
- Review the controls in place to ensure that ARs continue to have the necessary skills and knowledge to perform their duties.
- Assess the effectiveness of risk management strategies and controls.
- Review financial controls in place to prevent fraud and mismanagement.
- Review the protocols in place for data breach management and reporting.

Long term asset funds

The FCA's Long-Term Asset Fund ('LTAF') regime came into force on 15 November 2021, and is designed to facilitate investment in long-term, illiquid assets such as infrastructure, private equity, and real estate. The FCA has recently reiterated its intention to review the management of private market funds, which may now include operators of LTAFs, per the letter Asset Management & Alternatives Supervisory Strategy.

The LTAF regime is part of the FCA's broader effort to support access to, and investment in, long-term assets. Key features of the regime are:

Purpose

LTAF are designed to provide investors with access to long-term investments that are not typically available through traditional authorised funds such as UCITS and NURS. This allows for potentially higher returns associated with long-term investments.

Target investors

Originally designed solely for institutional investors, professional investors and sophisticated and high net worth retail investors, the FCA has now broadened the distribution rules for LTAFs to include retail investors receiving investment advice.

Liquidity management

LTAFs have specific rules for liquidity management to ensure that the funds can meet redemption requests while holding illiquid assets. In particular, LTAFs have a minimum 90 day notice period, and a dealing frequency of no more than 30 days. The redemption profile of the fund must be aligned with the liquidity of the fund's assets.

Governance and oversight

The LTAF regime includes robust governance and oversight requirements to ensure that the funds are managed in the best interests of investors. This includes requirements for detailed policies on valuation and risk management.

Disclosure requirements

Managers of an LTAF must provide comprehensive disclosures to investors about the nature of the fund's investments, the associated risks, and the terms of investment and redemption. This includes annual disclosures of how the fund has been managed in the interests of investors and quarterly statements setting out the investments held by the fund.

Valuations

LTAFs are subject to detailed valuation requirements, including the requirement to produce full quarterly valuations, and an indicative monthly valuation.

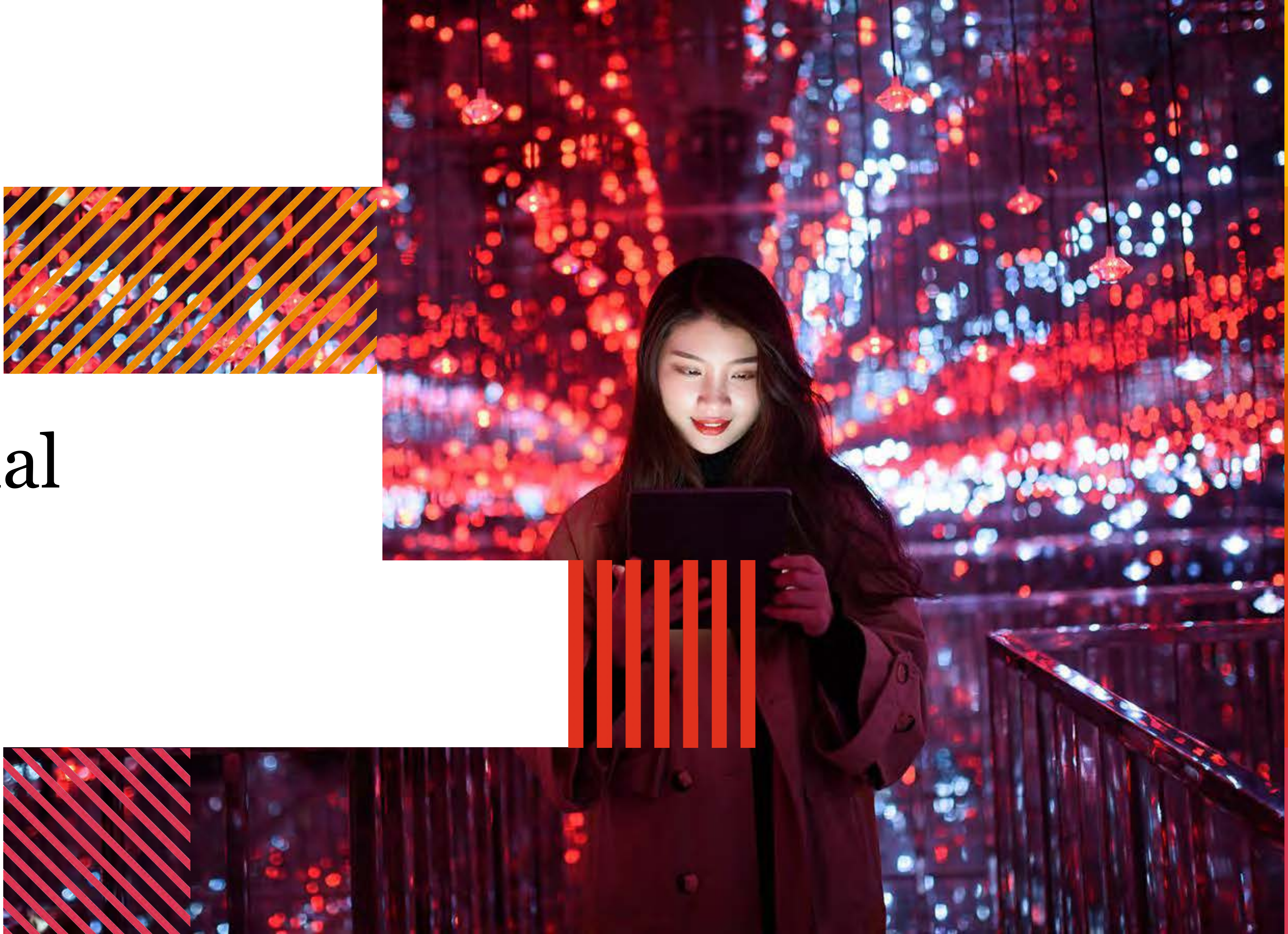
Key considerations for firms

- The FCA has reiterated its intention to review the approach firms are taking to the management of private market funds, including valuations, conflicts of interest and broader governance considerations. Operators of LTAFs need therefore to ensure that they can demonstrate compliance to the FCA.

Internal audit focus areas

- Review product governance and distribution strategies for alignment with both FCA regulations and the fund's offering documentation, including (where applicable) overlap with Consumer Duty.
- Review of product design process, with a particular focus on liquidity management and alignment of asset liquidity and redemption profile of the fund.
- Governance review to ascertain whether funds are being overseen appropriately and in line with FCA expectations.
- Review of the disclosures made to investors, including the annual and quarterly disclosures, to determine whether they meet the FCA's requirements and are likely to provide sufficiently clear and meaningful information to investors (in particular retail investors).
- Review of valuations policy and procedures against industry practice and FCA expectations.

Prudential matters



FCA insights on Internal Capital Adequacy and Risk Assessment (‘ICARA’)

The Investment Firm Prudential Regime (‘IFPR’) moves away from the old bank focused regime, and has introduced a more tailored regime for investment firms. However, the changes were substantial and required significant investment by firms, which continues as regulatory expectations evolve. The regime came into force on 1 January 2022.

By now, firms should have implemented the new rules, and should be focused on the new reporting elements – in particular the Internal Capital Adequacy and Risk Assessment (‘ICARA’). The FCA published findings from a thematic review in February 2023 looking at implementation by firms and then a further second thematic review in November 2023. Key findings included the need to focus on implementation where a firm is an investment firm group, the alignment of risk processes to the ICARA, wind-down planning, data quality and completeness and senior management oversight.

Background

The FCA has published their observations on how firms are implementing the IFPR in relation to the ICARA process and MIFID PRU reporting.

The FCA intend for firms to consider these findings alongside the FCA Handbook and other publications, namely the wind-down planning guide,

FG20/1 Guidance on assessing adequate financial resources, and TR22/1 Observations on wind-down planning.

Objective

The FCA has completed a multi-firm review. The review aimed to assess the progress of firms in adopting the new regime, including the conduct of their ICARA processes.

The review focused on capital and liquidity adequacy, and wind-down planning under the ICARA process, as well as regulatory reporting.

The FCA is continuing to conduct regulatory and liquidity capital and ICARA assessments with firms of all sizes as part of their business as usual (‘BAU’) activities.

Methodology

The FCA selected a sample of investment firms and groups covering various business models. The review included:

- Bilateral discussions with firms on risk assessment, threshold requirements, and the internal resource management frameworks.
- Reviewing ICARA documentation and other relevant information.
- Reviewing the quality of data submitted by each firm.

FCA focus areas

The key areas the FCA is focusing on include:

- Group assessments.
- Wind-down planning.
- Ongoing capital and liquidity requirements.
- Integration of risk management frameworks.
- Governance and responsibility.

FCA insights on ICARA (continued)

FCA observations

ICARA assessments

Some firms' ICARA analysis showed insufficient understanding of harms as risks assessed were not aligned to the risk management process.

Some firms did not adequately integrate their available risk tools to inform the ICARA process, including their risk appetite, risk indicator triggers, early warning indicators, and stress testing scenarios.

Firms did not provide the required information to explain any significant decrease in pre-IFPR financial requirements.

Boards did not provide sufficient challenge and oversight over the ICARA process.

Triggers and thresholds

Some firms used own funds and liquid asset appetite thresholds and triggers defined within MIFID PRU rules, without any link to the firm's understanding of its risk.

Some firms were not clear on whether their intervention points lead to discussions, trigger specific actions, or immediately set in motion tougher measures such as invoking the wind-down plan.

There was also insufficient use of reverse stress scenarios to test credibility of intervention points.

Where firm's Own Funds Threshold Requirements ('OFTR') / Liquid Assets Threshold Requirements ('LATR') were driven by wind-down resources, firms often did not have adequate resources to minimise harm.

Group ICARA process

The FCA observed that most investment firm groups opted to complete a 'group ICARA process'. However, they identified the following issues:

- There were instances where firms would not comprehensively consider the harm sustained by each firm individually.
- A group level assessment of resource requirements was, in some cases, inappropriately allocated to individual firms without clear reasons.

Without an entity-specific assessment, is it unlikely that the business will be able to comply with the overall financial adequacy rule (OFAR).

Next steps/key considerations for firms

1. IFPR training for Senior management and Board.
2. Internal audit involvement and challenge.
3. If firms have undertaken a group process, evaluate if solo firms have been assessed at the granular level.
4. Review risk management frameworks and identify where they align with IFPR, and can be amended to work collaboratively with the ICARA process.
5. Firms should undertake a detailed review of their metrics and thresholds and determine if they are appropriate.

Internal audit focus areas

- Assess the arrangements in place for the creation of the ICARA, including teams involved and their skills and capabilities.
- Review governance arrangements in place for the approval of the ICARA.
- Review the ICARA/specific sections of the ICARA against regulatory expectations and industry best practices.
- Review how management has assessed the FCA's published findings from their thematic review (February 2023 and November 2023; linked on the slide above) and implemented the relevant changes to their current ICARA.
- Review management's responses and actions taken to any specific regulatory feedback received on the firm's ICARA.

Valuation of assets

Assessment of value ('AoV') was introduced in September 2019 following findings from the asset management market study final report in June 2017. The AoV aims to improve competition in the sector and strengthen the duty of on fund managers to act in the best interests of investors. The FCA's recent thematic review (August 2023), and portfolio letter (March 2024), demonstrate the continuous focus of the regulator on AoV.

Authorised Fund Managers ('AFMs') are required to conduct an Assessment of Value ('AoV') at least annually on each share class of the UK authorised funds they manage. The AoV report must be published annually and must assess whether the fund's fees and charges are justified by the value provided to investors against a number of minimum considerations. AoV was introduced by the FCA to provide better protection to investors and improve competition in the sector.

The FCA conducted a thematic review on AoV and published its findings in August 2023. While some improvements were noted by the FCA compared to the previous review in 2021, there remain some areas for improvement.

The FCA key findings include:

01 **Gap analysis** – Some firms did not fully consider key findings/actions from their gap analysis and in some cases Directors were not involved in the gap analysis, leading to weaker AoV processes.

02 **AoV as business as usual ('BAU')**– Where firms had not integrated AoV processes in their product strategy and governance, this resulted in difficulties demonstrating a strong assessment of value.

03 **Impact of improved processes** – In some instances, although improved inputs were available to determine the assessment of value, they were ignored, often due to influence from group committees and Boards.

04 **Independent challenge** – The FCA found that, in some instances, Independent Non-Executive Directors ('iNEDs') did not provide challenge on the AoV methodologies or they were too involved in the collection and analysis of the information for the AoV, therefore comprising their independence.

05 **Quality of service assessment** – Areas for improvement were noted in relation to assessing quality of delegated managers' investment processes, including fees from these parties.

06 **Performance assessment** – The FCA noted some unrealistic and asymmetric measures to assess performance, including the assessment of underperformance compared to benchmarks.

07 **Economies of scale** – In some instances, the FCA found a lack of a detailed costing model or a large allocation of costs based on funds' relative assets under management, which would impact the cost analysis at a fund and share class level. Where economies of scale were achieved and reinvested in the business, the FCA noted concerns as to whether funds' investors were benefiting from these.

08 **Comparable market rates** – Comparable market rates is used in some instances as the justification for fees, even when other evidence from the minimum considerations would suggest otherwise. The FCA reiterated its stand that justifying fees based on comparable funds would not meet its expectations.

09 **Comparable services** – The FCA observed some areas for improvement in relation to discounted fees to some investors including whether other similar arrangements could be achieved with other affiliates/for other investors.

10 **Reporting** – Improvements were noted by the FCA in the AOV assessment conclusions and actions to remedy poor value.

The FCA's focus on AoV was re-iterated in its latest 'Portfolio letter' to asset managers in March 2024.

Valuation of assets (continued)

Internal audit focus areas

- Review the AoV assessment and the seven minimum considerations (quality of service, performance, costs, economies of scale, comparable market rates, comparable services and classes of units).
- Review of the governance arrangements and challenge around the preparation and approval of the AoV.
- Review of governance arrangements for product development and integration into BAU processes.
- Review of iNED roles and evidence of challenge.
- Review of reporting assessments and relative actions.
- Review of valuation practices for private assets, where applicable.

The Pensions Regulator (TPR)’s new General Code of Practice for pension schemes

The Pensions Regulator's (‘TPR’) General Code of Practice (the TPR Code) was published on 10 January 2024 and came into effect on 28 March 2024. The TPR Code combines 10 of TPR's existing codes into one document that outlines the regulator's expectations for the governance of occupational pension schemes. The TPR Code applies to the governing bodies of personal, public service, defined benefit (‘DB’) and defined contribution (‘DC’) occupational schemes.

- The new General code of practice (the TPR Code) was published by the Pensions Regulator (‘TPR’) in January 2024 to assist governing bodies of pension schemes in meeting their legal obligations and in ensuring their scheme is well governed.
- Employers have a key role to play in raising awareness of the TPR Code across occupational pensions schemes of all sizes. Topics of the TPR Code include: The effectiveness of internal controls, scheme risk management, consideration of ESG in implementing investment strategies, and cyber security risks.
- The TPR Code sets out the regulator’s expectations about the standards of conduct and practice expected of those they apply to. They are also designed to provide practical guidance on compliance with pensions legislation.
- The TPR Code of practice, previously known as the Single code of practice, combines 10 existing codes and introduces obligations not covered by the existing codes. It is intended to improve scheme governance and administration.
- The TPR Code applies to the governing bodies of occupational defined benefit (‘DB’) and defined contribution (‘DC’), personal, and public service pension schemes.

- The TPR Code provides the regulators expectations across a broad range of topics that stem from the management of a scheme and has 51 modules incorporated within the following five themes:

The governing body

Funding and investment

Administration

Communications and disclosure

Reporting to TPR

- Legal obligations referenced within the TPR Code include requirements to establish an effective system of governance (‘ESOG’) and, for those schemes with 100 or more members, to undertake an own risk assessment (‘ORA’). An ORA is an examination of how effectively the ESOG is working, and how any potential risks are being mitigated. This is the first time these legal obligations are referenced within a TPR Code of practice, so this is the first time TPR has set out its expectations on the establishment of an ESOG and the conduct of an ORA.
- The TPR Code also places emphasis on the importance of assurance and how schemes and their trustees consider obtain and use this in respect key risks impacting the scheme.

The Pensions Regulator (TPR)'s new General Code of Practice for pension schemes (continued)

Key considerations for funds

- **Governance and administration**: Ensure robust governance frameworks are in place, regularly review and update policies and procedures, and maintain accurate and up-to-date records.
- **Risk management**: Implement a comprehensive risk management framework, regularly identify, assess, and monitor risks, and ensure appropriate measures are in place to mitigate identified risks.
- **Cyber security**: Establish strong cyber security measures to protect data and assets, regularly review and update cyber security protocols, and train staff and trustees on cyber security best practices.
- **Trustee knowledge and understanding**: Ensure trustees have the necessary knowledge and skills to perform their duties, provide ongoing training and development opportunities for trustees, and keep abreast of legislative changes and industry developments.
- **Internal Controls**: Implement strong internal controls to safeguard scheme assets, regularly review and test the effectiveness of internal controls, and address any identified weaknesses or deficiencies promptly.
- **Environmental, Social, and Governance ('ESG') considerations**: Integrate ESG factors into risk management and investment decision-making processes, ensure compliance with relevant ESG regulations and guidelines, and communicate the scheme's approach to ESG to stakeholders.

Internal audit focus areas

- **Gap analysis:** Work with scheme management to assess the extent to which policies and procedures address the expectations of the Code, including a gap analysis of the Code against scheme operations.
- **Risk management framework:** Assess design of the framework, the extent to which the current framework supports the scheme in meeting the expectations of the Code and how it will support/facilitate the ORA process.
- **ORA readiness assessment:** Assess the draft ORA in line with regulatory requirements and industry good practice.
- **Assurance mapping:** Understand how management and the Trustees obtain assurance in respect of each section of the Code - identifying potential gaps.
- **Assurance framework:** Support the Trustees in developing an assurance framework that looks to address key risks as per the risk register and the expectations of the Code. Work with the trustees to determine the most effective approach to assurance including establishing a tailored and proportionate internal audit provision.
- **Deep dive assurance reviews:** Identify key risks and associated processes and assess the design and operating effectiveness of key controls (for example a deep dive review of cyber, investment and/or member administration controls).

Digital assets

Digital assets regulatory updates

2023

Travel Rule

The Travel Rule for crypto assets enters into force in September 2023.

Financial promotions

The financial promotion regime for crypto assets enters into force in October 2023.

Crypto framework

HM Treasury confirms the plans to regulate stablecoins and wider crypto assets in October 2023.

Fiat-backed stablecoins

Authorities issue discussion papers for a proposed regulatory framework for fiat-backed stablecoins in October 2023.

2024

Secondary legislation

Secondary legislation for fiat-backed stablecoins, crypto staking and wider crypto assets expected in 2024.

Digital securities sandbox

The initiative will help to facilitate the adoption of digital asset technology in the financial markets expected in 2024.

Fiat-backed stablecoins

Regulatory consultations issued for fiat-backed stablecoins expected in 2024.

2025

Digital pound

Design phase for a potential digital pound, ongoing until 2025/26.

Fiat-backed stablecoins

Final rules expected for implementation.

Wider crypto assets

Regulatory consultations expected in 2025.

Wider crypto assets

Final rules implemented in 2025, at the earliest.

Digital pound

Decision on whether to progress to a digital pound build phase to be made in 2025, at the earliest.

The EU's Markets in Crypto Assets Regulation (MiCAR):

30 June 2023 - MiCAR's entry into force

30 June 2024 - rules apply for stablecoins

30 December 2024 - final regulatory technical standards

30 June 2026 - transition period ends

Note: Some dates are subject to change due to the change in the Government.
Further information available in the FCA's Regulatory Initiatives Grid, as published twice a year.

Digital assets – Emerging regulatory frameworks

The UK authorities remain committed to setting up a clear regulatory regime for digital assets, including fiat-backed stablecoins and wider crypto assets, as well as supporting the FS industries tokenisation efforts.

Crypto asset regulatory developments

The Financial Services and Markets Act 2023 ('FSMA 2023') provides the authorities with powers to specify crypto asset activities within the FSMA 2000 Regulated Activities Order 2001 ('RAO'), and to designate activities as part of the Designated Activities Regime ('DAR'). FSMA 2023 also gives authorities powers to deliver a regulatory regime for the use of 'digital settlement assets' (DSA), e.g. stablecoins, in payments.

The new regime will capture all crypto assets. The requirements will be determined by the activities firms undertake and are primarily delivered by amendmending the existing legislations.

All financial entities undertaking crypto asset activities will be impacted, including those already registered with the FCA. Firms will need to comply with compliance responsibilities, including conduct and prudential requirements, safeguarding, reporting, consumer protection, market abuse, operational resilience and location policy.

Asset classification framework

The UK authorities will apply a phased approach to regulating digital assets, expected to come into effect in 2025, at the earliest.

- Phase 1: Fiat-backed stablecoins used for payments, including issuance, payment and custody.
- Phase 2: All other tokens, when used for regulated activities, including issuance, exchange, investment and risk management, lending, borrowing and leverage, as well as custody.

The in-scope crypto assets will include exchange tokens (e.g. cryptocurrencies), asset-referenced tokens, commodity-linked tokens, crypto-backed tokens, algorithmic tokens and governance tokens, as well as non-fungible tokens ('NFTs'), utility tokens and fan tokens (where used for regulated activities).

The regulatory frameworks for decentralised finance ('DeFi') activities will be considered at a later stage.

Registration/authorisation

Currently, crypto asset firms must comply with the money laundering, terrorist financing and transfer of funds (information on the payer) regulations 2017 ('MLRs'). Firms are required to register with the FCA before conducting business or notify the regulator before a proposed acquisition of a registered crypto asset firm.

Under the new regime, firms undertaking regulated activities must adhere to the same financial crime standards and rules which apply to equivalent or similar traditional FS activities.

Firms already registered with the FCA will also need to seek authorisation from the FCA, under the new wider regime.

For more information, see PwC's Global Crypto Regulation 2024 Report.

Digital assets – Emerging regulatory frameworks (continued)

Financial promotion of crypto assets

The FCA classifies qualifying crypto assets as ‘restricted mass market investments’ under the Financial Promotions Order (‘FPO’). Since October 2023, firms marketing qualifying crypto assets to the UK customers must be registered with the FCA under the MLRs, irrespective of the firms’ location or the technology used to make the promotion.

The financial promotion must be either:

- Communicated by an authorised person, made by an unauthorised person but approved by an authorised person, communicated by (or on behalf of) a crypto asset business registered with the FCA under the MLRs; or
- Communicated in compliance with the conditions of an exemption in the FPO.

Firms must also comply with a further set of ‘back end rules’, such as personalised risk warnings, a 24-hour cooling-off period, client categorisation, and appropriateness assessments.

In August 2024, the FCA published a review on the back end rule compliance. The regulator warns firms against relying on industry comparisons to benchmark what is acceptable, given the prevalent poor practices in the market.

Fiat-backed stablecoins

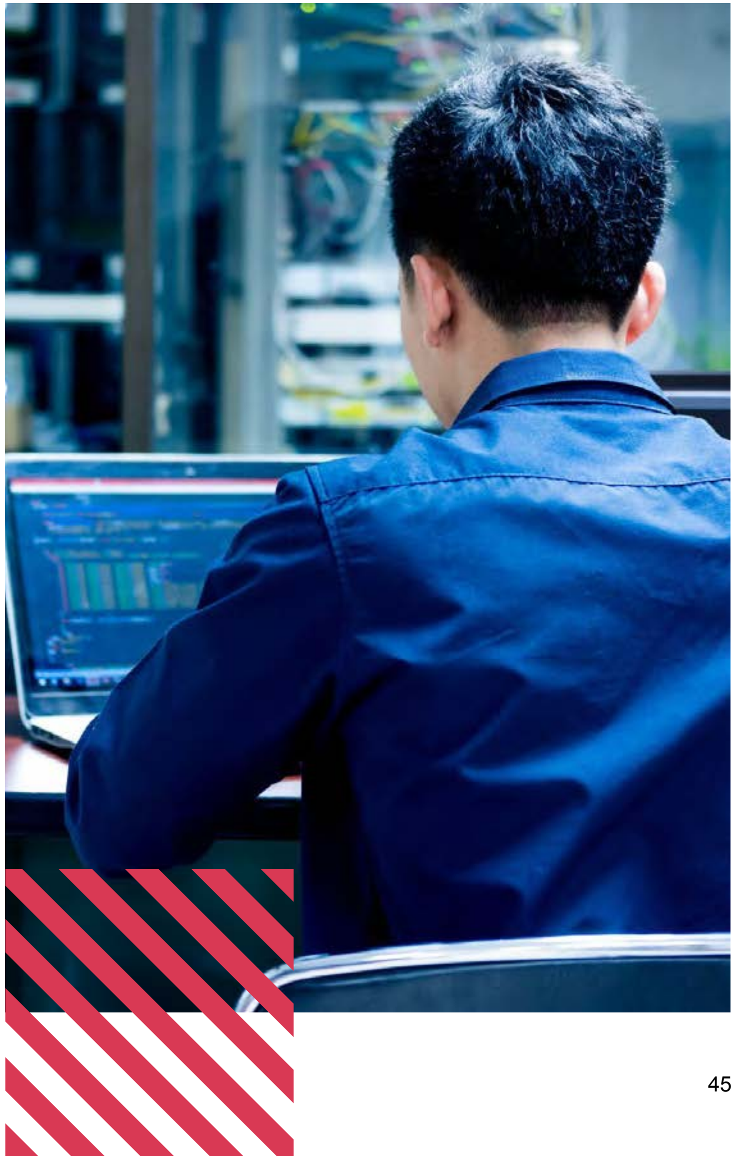
The new regime for fiat-backed stablecoins is expected to come into force in 2025, at the earliest. The framework will bring certain stablecoin activities under the regulatory perimeter, namely issuance of fiat-backed stablecoins in or from the UK, and custody activities carried out from the UK or to UK based consumers for UK-issued fiat-backed stablecoins. HM Treasury will also amend the Payment Services Regulations 2017 (‘PSRs’) to allow fiat-backed stablecoins to be used as a means of payment.

Issuers will need to constitute and maintain a reserve of backing assets, equivalent in value to the circulating supply of the regulated stablecoin, together with adequate safeguarding arrangements.

For custody, the core requirements include arrangements to protect clients’ rights to their crypto assets, organisational arrangements to minimise risk of loss or diminution of clients’ custody assets, accurate books and records of clients’ custody assets holdings, and adequate controls and governance to protect clients’ custody asset holdings.

The FCA will apply the same or equivalent organisational requirements to regulated stablecoin issuers and custodians, as in place for traditional finance firms. The regulator also plans to issue a dedicated prudential sourcebook for regulated stablecoin issuers and custodians, applied cumulatively with other activity-based prudential requirements.

The BoE will supervise systemic, stablecoins, which are used for retail purposes in the UK. The regime will apply to systemic payment systems using stablecoins, systemic service providers to payment systems using stablecoins and other service providers.
The rules for stablecoins will later apply to wider crypto asset activities.



Digital assets – Emerging regulatory frameworks (continued)

Digital pound

The BoE and FCA have indicated that a retail digital pound is likely needed by 2030. The work on a retail digital pound is one part of the BoE and HM Treasury's efforts to ensure that the UK remains at the forefront of innovation in money, payments and digital finance.

The digital pound is in the design phase, with a focus on technology and policy options. The decision on whether to progress to the build phase will be made by the authorities in 2025, at the earliest. In May 2023, the Government committed to introducing primary legislation before launching a central bank digital currency ('CBDC'), preceded by a further public consultation.

For more information, see PwC's comparative report on digital pound, euro and krona as well as on the BoE's discussion paper on its approach to innovation in money and payments, published in July 2024.

Tokenisation

Tokenisation, the process of issuing a digital unique and anonymous representation of a real asset (e.g. a real-world or digital asset), on a blockchain, has the potential to open up new revenue streams, speed up operations and cut costs.

The FCA and HM Treasury are working with the industry and global authorities to explore potential uses of tokenisation, with an immediate focus on fund tokenisation. According to the FCA, fund tokenisation could make collective investment schemes more efficient, transparent, and accessible to a wider range of consumers.

The authorities are set to establish a digital securities sandbox in 2024, to further drive the opportunities within tokenisation. For more information, see PwC's analysis on tokenisation in financial services.

Next steps

01 For fiat-backed stablecoins, the Government is expected to bring forward the secondary legislation in 2024, to enable the FCA's regulatory powers. The authorities are expected to develop regulatory rules for consultation by 2025. The stablecoin regime will be implemented in due course after.

02 For wider crypto assets (phase 2), the expected timelines for the secondary legislation and regulatory rule setting will follow soon after phase 1.

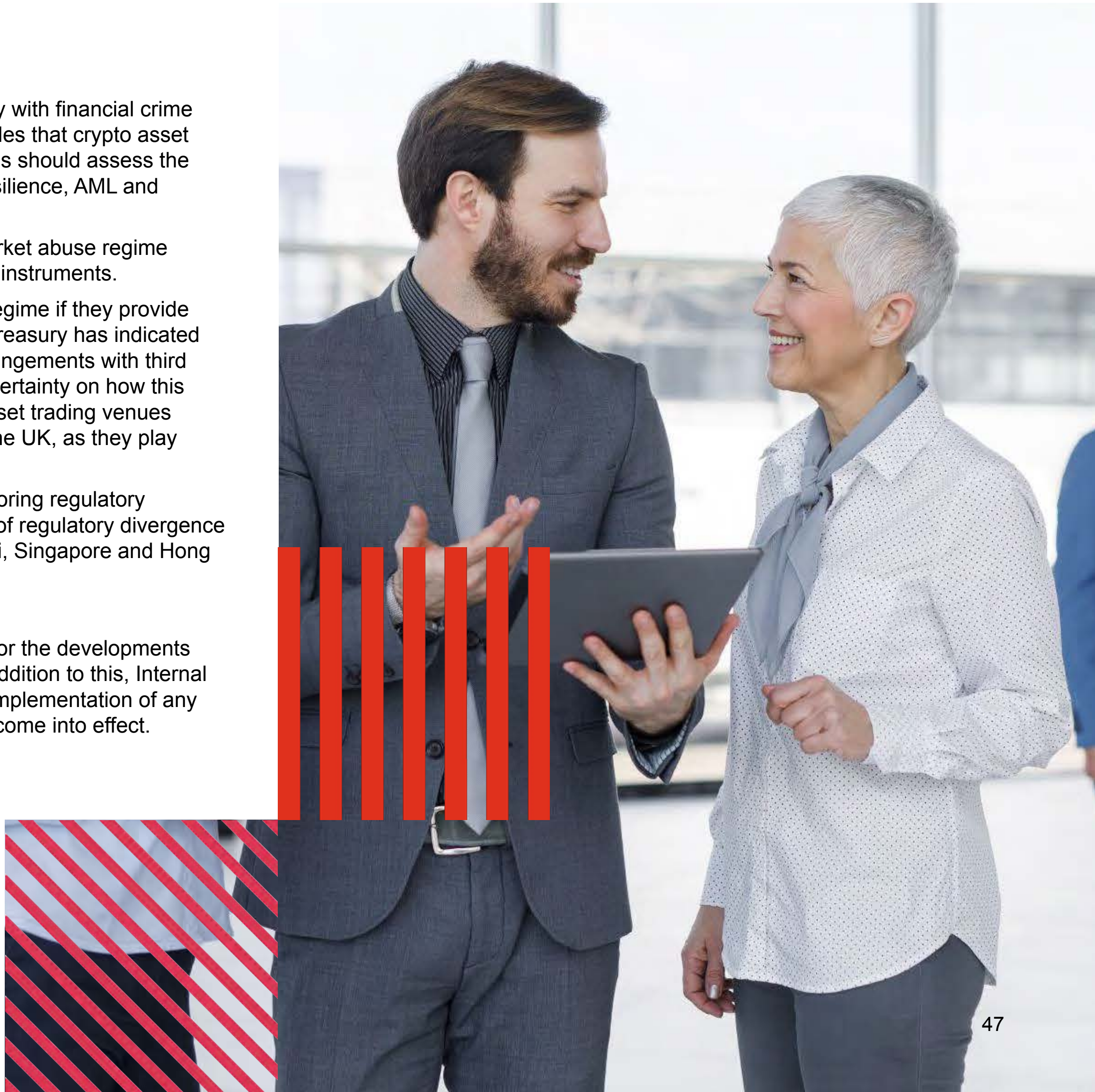
03 The decision on whether to progress to the build phase of digital pound, will be made in 2025, at the earliest.

Digital assets – Emerging regulatory frameworks (continued)

Key considerations for firms

- All FS firms should evaluate the potential impact of the proposed regimes on their strategy and operations.
- Practices and regulatory guidance surrounding asset classification, measurement requirements, fair value considerations, disclosures and other issues are progressing with the upcoming consultations. As the regulatory expectations become clearer, financial institutions, corporations and consumers are better enabled to opt in to the rapidly expanding industry.
- Firms which already carry out crypto asset activities should map out current activities against the proposed regime, assessing business model implications and implementing new processes and arrangements to ensure compliance with the new regime. These include governance, controls, and oversight frameworks put in place to manage any crypto asset or stablecoin arrangements.
- Some firms will need to apply for an authorisation under FSMA as part of the new regime. Firms should note that authorisation under the current AML/CTF regime has been challenging and that only a minor percentage of applications have been approved by the FCA.
- Firms which are already FSMA authorised and intend to undertake some newly regulated activities will generally need to apply for a variation of permission from the FCA (and the PRA for dual-regulated firms). Regulatory permissions will not be automatically granted for firms which are already authorised.
- Under the proposals, firms will need to comply with financial crime rules in FSMA. These are broader than the rules that crypto asset businesses already need to comply with. Firms should assess the design and robustness of their operational resilience, AML and CTF frameworks.
- Firms will also need to comply with a new market abuse regime based on elements of the regime for financial instruments.
- Overseas firms will need to comply with the regime if they provide services to customers based in the UK. HM Treasury has indicated that it intends to pursue equivalence type arrangements with third countries. However, there is considerable uncertainty on how this model will develop. Firms operating crypto asset trading venues would be likely to require subsidiarisation in the UK, as they play a critical role in the crypto asset value chain.
- Firms should also review processes for monitoring regulatory developments and identifying possible areas of regulatory divergence between jurisdictions, including the EU, Dubai, Singapore and Hong Kong, where relevant.

Internal audit functions should continue to monitor the developments relating to emerging regulatory frameworks. In addition to this, Internal Audit should provide assurance over the firm's implementation of any new regulatory requirements as and when they come into effect.



Technology and operations

Cyber

Cyber crime continues to be an agnostic and pervasive threat, affecting all countries and sectors through a variety of techniques to achieve the common goal of monetising access to firms and their data. Critical to the economic fabric of society, FS firms are a high value target for cyber attacks, with their attack surface broadening as the sector increasingly innovates, digitises its operations, and embraces fintech.

Industry trends and insights*

Key findings from the 2024 Global Digital Trust Insights Survey:

- **Top risks –** Digital and technology risks, and cyber risks – are intertwined, requiring CISOs and tech leaders to position themselves at the epicenter of innovation in their firms.
- **The proportion of costly cyber breaches ($1m+) has increased** since last year.
- **Cloud –** Most concerning threat (47%) to firms and top priority for cyber investments (33%) and yet challenging for firms to manage.
- **Cyber investments remain a priority –** Modernisation and optimisation top the cyber investment priorities for 2024.
- **Simplification underway -** Movement to integrated tech solutions or suites is increasing.
- **DefenseGPT -** Firms are starting to deploy generative AI tools for cyber defence.
- **Regulation -** Business and tech leaders see various regulations as helpful to securing future growth. Anticipate additional compliance costs and significant business transformation.
- **Top performing firms** - Which display greater maturity in their cyber security initiatives, report a greater number of benefits and a lower incidence of costly cyber breach of $1m+, or a breach at all.

* See linked here | **PwC Global Digital Trust Insights Survey 2024**

This annual survey captures the views of business and tech leaders around the world on the challenges and opportunities to improve and transform cyber security in their firm in the next 12 to 18 months.

Cyber threats – A year in retrospect summary**

Recurring themes in the threat environment

Zero days, critical vulnerabilities, supply chain and cloud compromises have challenged firms across all sectors, with more vulnerabilities disclosed in 2023 than ever before.

Geopolitical conflicts and tensions around the world have increased. Threat actors – particularly of espionage, sabotage, and hacktivism motivations – continuing to react and respond, shifting direction and broadening their activities.

Threat actors will leverage what works, continuing to use known methods in addition to shifting techniques for more effective campaigns, adjusting for emerging technology and increased use of cloud services.

Ransomware and extortion continued to be a significant issue, as leak site victims reached record levels in 2023.

** These insights draw upon analysis conducted by the PwC threat intelligence team across 2023 and reported on in the latest Year in Retrospect, and which we continue to see across the threat landscape in 2024.

Cyber (continued)

Internal audit focus areas

Based on lessons learned across industry, the following is a set of key focus areas and expected controls, which internal audit can consider when evaluating cyber resilience:

Protection of the IT environment

- Multi-factor authentication (‘MFA’) configured for all email and remote access accounts.
- Web security tooling that restricts content and blocks malicious downloads.
- Email tooling that restricts attachments and scans for malicious content.
- Hardened endpoints to restrict execution of untrusted scripts and executables.
- Restrictions that prevent the execution of untrusted Microsoft Office macros.

Early detection of potential threats

- Endpoint Detection and Response (‘EDR’) tooling deployed on workstations and servers.
- Continuous monitoring capability that rapidly investigates and contains alerts, including out of hours.
- Regular ‘red teaming’ to validate detection and response capabilities.

Prevention of unauthorised access

- Controls to restrict and secure the use of accounts with domain administrator privileges.
- Internal vulnerability scanning with effective remediation processes.
- Proactive hunting and remediation is conducted in relation to Active Directory hygiene issues.
- Host-based firewalls on workstations are configured by default to block inbound traffic.
- Outbound Internet access for all servers is restricted to allow-list by firewalls and web filtering tools.

Cyber incident response and recovery

- Exercised cyber incident response and crisis management plans are in place.
- Playbooks are established for rapidly isolating parts of network and managing the impact.
- Validated backups with tested recovery of infrastructure (e.g., Active Directory) are in place.
- Prioritised recovery plans are in place for key business systems and applications.

Resilience, Response and Recovery from major disruptions

Recent industry IT outages underscore a fundamental truth: the digital age, while transformative, is fraught with risks that can disrupt even the most well-prepared firms. In the following section we delve into more detail around how critical third parties (‘CTP’s), cloud, AI and digital transformation all impact a firm’s ability to remain operationally resilient.

Key considerations for firms

- Business resilience requires **continuous evolution** to protect against shocks, adapt, create value, and maintain a competitive edge.
- Traditional, siloed approaches lead to fragmented and ineffective crisis responses. Firms must integrate core resilience competencies and leverage technology to achieve a **unified view of events and enable a coordinated, effective response to disruptions.**
- A well-coordinated response to IT disruptions extends beyond IT teams, requiring **organisational alignment and strategic decision-making.**
- Firms need to **prepare and test for major incidents** that inflict more damage to their technical environment without which recovery is not certain.
- A successful Cyber ransomware attack presents responders with far a more **severe challenge** as it logically destroys an environment leaving the only route back a complicated and slow recovery from a compromised backup. **Lessons from Cyber Recovery** have a key role to play in guiding secure recovery from accidental IT disruption.
- Recent industry outages underscore the critical need for enhanced **collaboration** between Third Party Risk Management (‘TPRM’), IT, and service owners. TPRM professionals need to work closely with IT to better understand digitisation, product development, and the technology architecture that underpins **critical business services**.

Internal audit focus areas

Technology resilience

- Management’s understanding of critical business service interactions, dependencies on enabling services and identification of those that can disable the firm if they fail.
- Effectiveness of change management processes and testing regimes.
- Effectiveness of incident management and cyber recovery processes.

Digital supply chain vulnerabilities

- Mapping of supply chains to show service delivery and third-party interactions. Understanding of contractual clauses relating to incidents.
- Effectiveness of risk assessment and due diligence processes over critical suppliers.
- Processes in place to stress-test contingency plans to ensure robust response capabilities.

Effective crisis response

- Effectiveness of response plans and testing, including crisis exercises to validate and enhance response frameworks.
- Consideration of joint exercises, war games and/or scenario tests with CTPs to embed and rehearse a joined up response capability, and identify vulnerabilities which may impact critical service provision in the event of future outages.
- Management’s understanding of the role of insurance to respond to major IT disruptions.

Operational resilience

Operational resilience continues to be a pivotal priority as firms strive to fulfill regulatory mandates by March 2025. As this deadline approaches, emphasis is on not only achieving compliance but also ensuring that operational resilience programmes are robust, resilient, and capable of adapting to future challenges to secure long-term stability and trust.

December 2019
Consultation Paper published

October 2020
Consultation closed

March 2021
Policy statement publication

March 2022 – March 2025
Time to take action to demonstrate ability to remain within impact tolerances

Post March 2025
Innovate and embed into business as usual (BAU)

Key considerations for firms

Enhanced testing regimes

- **Testing sophistication:** Development of more complex testing scenarios, including those impacting multiple Integrated Business Services ('IBS') and end-to-end testing of individual IBS.
- **Testing intensity:** Conducting rigorous testing, including scenarios that seek to push systems to failure and beyond impact tolerance thresholds.
- **Testing integration:** Alignment of testing activities with other firm-wide testing initiatives, such as crisis and business continuity treatment plan testing.

Vulnerability management

- **Vulnerabilities identification:** Implementation of robust identification processes integrated with IBS evaluation, mapping, incidents management, and risk assessments.
- **Tracking vulnerabilities:** Development of a centralised system or platform for tracking identified vulnerabilities, remediation efforts, and any attendant feedback loop.
- **Remediating vulnerabilities:** Implementation of a range of mitigation strategies tailored to the specific nature of the vulnerability.

Re-validation

Review and refresh of IBS prioritisation, mapping, Impact Tolerances ('ITOLs'), and the scenario library to ensure that these processes remain dynamic and reflective of current realities.

Resilience reporting

- **Metrics and triggers:** Establishment of relevant and actionable resilience metrics and indicators that track resilience across the key resilience resource pillars to improve the quality and depth of management information ('MI').
- **Internal reporting**: Establishment of effective internal reporting structures to enable Board and senior management to make more informed, timely, and effective decisions concerning investments, operational directions, and risk exposure.
- **Self-assessment:** Comprehensive self-assessment processes, including vulnerability reporting and remediation plans extending beyond 2025 (where required).

Tooling/technology

The focus on tooling is becoming paramount as firms begin to transition resilience into BAU. Firms are already leveraging advanced tools and technology to gain rapid insights into disruptions. The best resilience tools are utilising capabilities that enable quick responses to incidents and immediate recovery.

Operational resilience (continued)

Looking beyond March 2025

Post-March 2025, the focus will start to shift towards the continuous enhancement and sophistication of operational resilience approaches. A critical area will be instances where there are **outstanding vulnerabilities** that have not been addressed during the transitional period. These will need to be addressed as a matter of priority as the deadline requires firms to be able to operate within impact tolerances for severe but plausible scenarios, and outstanding vulnerabilities compromise the ability to do that.

There will be a strong emphasis on the **evolution of tooling and technology**. The commitment to advancing resilience through the continuous improvement of tools and technologies is paramount. This includes adopting innovative solutions that can provide quicker insights and more effective responses to disruptions.

Additionally, **long-term strategies will need to be developed** to maintain and enhance resilience in alignment with evolving business priorities. These strategies will help ensure that firms remain proactive in their approach to operational resilience, adapting to new challenges and maintaining stakeholder trust.

This period will also no doubt provide firms with **greater flexibility to demonstrate innovation in embedding operational resilience into BAU**. Depending on specific operational contexts, firms can develop and implement creative solutions that enhance their resilience framework while meeting regulatory standards.

Internal audit focus areas

- Ensure that the identified IBS and their impact tolerances are regularly reviewed, updated, and validated.
- Assess the comprehensiveness of service mapping in terms of depth and breadth.
- Assess the complexity and thoroughness of testing scenarios, including those impacting multiple IBS and end-to-end testing.
- Review the intensity of testing, such as testing to failure and beyond impact tolerance thresholds.
- Ensure alignment and integration of testing activities with other firm-wide initiatives, like crisis management and business continuity.
- Evaluate the processes for identifying, tracking, and mitigating vulnerabilities.
- Verify the effectiveness of action plans in addressing vulnerabilities and linking improvements to resilience.
- Validate the relevance and actionability of metrics and indicators used for internal and external reporting.
- Ensure the effectiveness of internal reporting structures and decision-making processes.
- Review self-assessment processes, including vulnerability reporting.

Digital Operational Resilience Act ('DORA')

'DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of Information and Communication Technology ('ICT') related disruptions and threats.' – Council of the EU

What is DORA?

DORA is a new European regulation that comes into force on the 17 January 2025 and defines detailed and comprehensive regulations for digital operational resilience at the EU level. Its key objectives are to:

01 **Harmonise local regulations** in the financial sector across the EU member states.

02 Ensure that financial entities and Third-Party Providers ('TPP'), **respond to and recover from all types of ICT-related disruptions** in a **timely and appropriate manner.**

03 **Improve** ICT risk management.

04 Empower financial supervisory authorities to **monitor and audit** financial entities and their third-party ICT providers more closely.

05 Standardise **incident reporting mechanisms and knowledge sharing.**

Scope of DORA

DORA's **scope of application** encompasses traditional financial sector entities such as credit institutions, exchanges and clearing houses, alternative fund managers, insurance companies, payment institutions, electronic money institutions, as well as crypto-currency, crypto-asset issuers and token issuers.

Whilst this is an **EU regulation**, it will have an impact on **non-EU entities with operations in the EU** (including provision of intragroup ICT/Cyber services to EU countries), and **critical third-parties** ('CTP's) that provide services to EU-based entities. DORA's scope extends to include other stakeholders in the financial sector, which so far have not been subject to extensive ICT security regulation.

The regulation also introduces a **Union-wide oversight framework on critical ICT third-party providers**, who will be designated by the ESAs in 2025.

If requirements are not met local EU regulators (known as 'competent authorities') can:

- Demand specific actions be taken to remediate vulnerabilities.
- Impose administrative penalties.

Digital Operational Resilience Act (‘DORA’) (continued)

Key considerations for firms

The DORA directives covers 5 key areas/pillars that are relevant for the reporting entities. The following outlines key considerations for firms:

01 ICT risk management

- The **ICT risk management framework** must be detailed and aligned with the corporate strategy and objectives.
- A **strategy for digital resilience** must be defined.
- **Enhance first line of defense capabilities**, from threat detection to response, recovery, and communications, with emphasis on – but not limited to:
  - Threat scenario modeling.
  - Cyber protection and prevention.
  - Business continuity and disaster recovery communication.

02 Digital operational resilience testing

Digital operational resilience testing

- **Annual testing** of all critical ICT systems.
- Advanced **threat-led penetration testing** every 3 years.
- Involvement of **ICT third-party** providers.

03 Incident management

- Integration into ICT **risk management framework**.
- Essential **contractual requirements.**
- Keeping an information register on **all services provided by ICT third parties.**
- **Reporting on changes** in the use of critical ICT services.
- Assessment of **ICT concentration risk** and **sub-outsourcing.**
- Restricted use of third-party ICT providers **in third countries.**

04 Information sharing

- **Reporting** of ICT-related incidents (and significant cyber threats).
- Submission of **initial, interim, and final reports** on serious ICT-related incidents (and significant cyber threats).
- Conducting a **root cause analysis** after ICT-related incidents.
- Identification and **reporting of required improvements.**

05 ICT third-party risk

- **Sharing cyber threat intelligence** and insight to improve digital operational resilience.
- **Agreements** on the exchange of information (including conditions for participation).
- Implementation of **mechanisms to review and take action** on the information shared by the authorities.

17 January 2025
In-scope entities will be expected to be compliant with DORA.

Digital Operational Resilience Act ('DORA') (continued)

DORA identifies a number of specific requirements for Internal audit to perform. In addition, internal audit has a key role to play in support of DORA compliance, both in assessing a firm's plan for compliance, and through providing assurance over key areas in scope for DORA.

DORA - Impact on internal audit

DORA identifies a number of specific requirements that impact internal audit:

Article 5

- The management body shall: approve and periodically review the financial entity's **ICT internal audit plans, ICT audits and material modifications to them**.

Article 6

- The **ICT risk management framework** of financial entities (other than microenterprises*), **shall be subject to internal audit** by auditors on a regular basis in line with the financial entities' audit plan.
- Based on the conclusions from the internal audit review, financial entities shall establish a formal follow-up process, including rules for the **timely verification and remediation of critical ICT audit findings**.

Article 11

- As part of the ICT risk management framework referred to in Article 6(1), financial entities shall implement associated **ICT response and recovery plans** which, in the case of financial entities other than microenterprises*, **shall be subject to independent internal audit reviews**.

* Microenterprises have reduced compliance requirements within DORA. The varying applicability to microenterprises is specifically addressed within the relevant sections of the Act.

Internal audit focus areas

DORA programme assurance

The **scale and complexity** of a programme that seeks to **implement a resilience approach** that aligns with DORA requirements is such that there will be a variety of challenges over the course of the implementation.

Internal audit can provide benefit to a business's DORA compliance by providing **assurance over the programme of work**.

The following are examples of assurance activities that may be performed by internal audit:

- Checking that planned **activities address the DORA requirements** and are appropriately **resourced and phased**.
- Deep dives focussed on the **development of specific artefacts and outcomes** required for DORA compliance. For example, the approach to mapping critical or important functions.
- Assessing whether the **governance, people, processes and technology** are in place to support DORA compliance (including the ability to generate the artefacts expected by DORA, such as the ICT Risk Management Framework Review report).
- **Validating remediation activities** over identified gaps against the DORA requirements.

DORA component audits

DORA brings together a **wide range of business activities** that support operational resilience. These activities are often discrete and internal audits may be performed over these areas, with the associated priority within an audit plan of such areas being raised by the associated regulatory requirements.

Audits of these discrete areas may include, but are not limited to, coverage of:

- **Incident Management**: Under DORA this would include consideration of the process, approach and documentation around incident reporting and loss estimation/measurement.
- **Threat Led Penetration Testing**: DORA specific activities would include the approach to reporting on outcomes to different European Regulators.
- **Digital Operational Resilience Testing Strategy**: Areas assessed could include the approach for integrating testing outcomes, planning remediation and governing the process.
- **Third Parties**: DORA specific artefacts include an ICT third-party risk management strategy and concentration risk assessment. A register of information ('ROI') will need to be created and maintained and contracts will require appropriate clauses aligned with DORA requirements. Exit plans will also need to be created and periodically tested for ICT services supporting critical or important functions.

Third party risk management (‘TPRM’)

Reliance on third party service providers continues to grow as firms embrace digitisation and scale their operations whilst reducing costs. The scope of reliance on third parties has expanded significantly so that firms’ critical or important business processes and functions are often underpinned by at least one third party and, in many cases, subcontractors as well. The inherent complexity of the digital supply chain poses significant resilience challenges. Firms must adopt a ‘resilience by design’ approach, emphasising comprehensive understanding and proactive management of third party dependencies.

A number of key challenges continue to arise in relation to third party risk management. Some of these are relate to meeting **DORA** compliance in January 2025 as highlighted below (also see DORA section within this pack):

- Developing and defining a method for identifying critical or important functions that can be applied consistently across the firm’s group (i.e. in a number of firms there will be multiple entities in-scope for DORA but these may vary in both size and complexity).
- The ability to gain an accurate understanding of the full suite of ICT services that are provided by third parties (including intragroup) and which of these ICT services support critical or important functions.
- Navigating the complexities of contractual arrangements with ICT third-party service providers, including the need to include DORA-specific clauses (large technology providers tend to contract on their own terms) and re-papering complex global contracts (i.e. Master Service Agreements) that are held outside of in-scope jurisdictions as part of intragroup arrangements.

Regulatory oversight and horizon scanning will continue to be important to enable firms to take a proactive approach to meeting compliance requirements, particular focus and consideration should be given to:

- Corporate Sustainability Due Diligence Directive (‘CSDDD’) aims to ensure that companies operating within the EU adhere to **sustainable and responsible business practices.** The directive seeks to address human rights and environmental impacts throughout the supply chain of companies by imposing due diligence obligations.
- **Critical Third Parties (CTP)**: an extension of the FCA’s efforts to address systemic risks posed by certain third parties to the UK financial sector (please see page 58 for details).

[1] ECB Outsourcing register: Annual horizontal analysis (21 February 2024)

UK critical third parties regime

The UK Critical Third Parties ('CTP') regime aims to bolster the operational resilience of the FS sector through increased regulatory expectation on key third-party service providers, including prominent cloud providers. This introduces additional compliance and operational demands on those designated by the His Majesty's Treasury (HM Treasury) as CTPs and will have associated impacts on their clients and supply chains.

July 2022
Discussion paper DP3/22 lays out principles of the proposed approach.

July 2023
Amendment to FSMA grants regulators necessary legal powers.

December 2023
Consultation paper CP26/23 launches with draft rules.

March 2024
Close of consultation period on draft rules.

Q4 2024
Possible final rules and first designation of CTPs by HM Treasury three months later.

H1 2025
Possible first self-assessments then due three months after designation.

Early 2026
First annual self-assessments demonstrating compliance due.

Key considerations for firms

What is the CTP regime?

The Critical Third Parties ('CTP') regime in the UK will introduce direct supervision by the Bank of England ('BoE'), the PRA, and the FCA of **critical third-party service providers** to UK firms and FMIs, which will include Cloud Service Providers ('CSPs').

Third-party service providers designated as a CTP will have a significant new set of regulatory obligations they must comply with, which in turn will impact the other third parties in their supply chains.

While in the regime no service providers have yet been designated as a CTP, it is near-certain that cloud hyperscalers will be included.

Regulatory requirements

As part of the CTP regime, there are **6** fundamental rules which CTPs must comply with, as well as **8 Operational Risk and Resilience ('OR&R') requirements** in the following areas:

1. Governance.
2. Risk management.
3. Dependency and supply chain.
4. Technology and cyber resilience.
5. Change management.
6. Mapping.
7. Incident management.
8. Termination of services.

How will HM Treasury identify the CTPs?

HM Treasury has the power to designate persons who provide services to UK FS firms and FMIs as CTPs if satisfied that **'a failure in, or disruption to, the provision of those services … could threaten the stability of, or confidence in, the UK financial system.'**

On identification of CTPs, HM Treasury may consider the following criteria:

- The materiality of the services the third-party provides to firms and FMIs.
- The number and type of firms and FMIs which use a third party.

The regulators will provide recommendations to HM Treasury for which firms should be designated.

ICT third-party risk

What does this mean for regulated firms?

Firms must continue to comply with their existing regulatory obligations under SS2/ 21 – operational resilience and SS1/21 – third party risk management.

Firms should engage with their CSPs on the regulatory ask (if not already doing so) to be able to give clarity to their regulators about resilience in the cloud.

In the longer term, firms may benefit from:

- Greater transparency from their third parties in scope of the regime.
- Access to incident reports.
- Participation in financial sector incident management exercises.

UK critical third parties regime (continued)

Internal audit focus areas

Based on publicly available information to date, we do not expect firms to be required to treat CTPs any differently from other material service providers. Within the TPRM process, some areas that will benefit from specific attention from an internal audit perspective include:

Third-party Risk Management Framework:

- The effectiveness of third-party risk management policies and procedures.
- The effectiveness of the due diligence process for onboarding and ongoing monitoring of material third party service providers.

Contractual Agreements:

- The approach to contracts with material third party service providers to ensure they include clauses that address regulatory requirements, data protection, service level agreements ('SLAs'), and exit strategies.
- Provisions for regular audits and assessments of material third party service providers.

Resilience and Business Continuity:

- The firm's own resilience plans in the event of a failure or disruption involving a material third party service providers and ensure these plans are tested regularly.
- How the firm will make use of self-assessments received from those material third party service providers who are designated as CTPs.

Incident Management

- Incident management procedures related to material third party service providers.
- Processes for reporting, investigating, and mitigating incidents involving material third party service providers.
- Handling of incident notifications received from material third party service providers who are designated as CTPs.

Cloud risk

FS firms face unique challenges when embarking on the journey to unlock the full potential of cloud technology, given the intense regulatory scrutiny of cloud adoption and the need to demonstrate they are embedding resilience at the heart of their technology architecture. Successfully navigating these challenges requires an holistic approach that addresses regulatory, security, technical, operational, and organisational aspects of cloud adoption.

Key considerations for firms

Regulatory Compliance - Securing both regulatory and internal policy approval for migrating critical services or workloads to the Cloud.

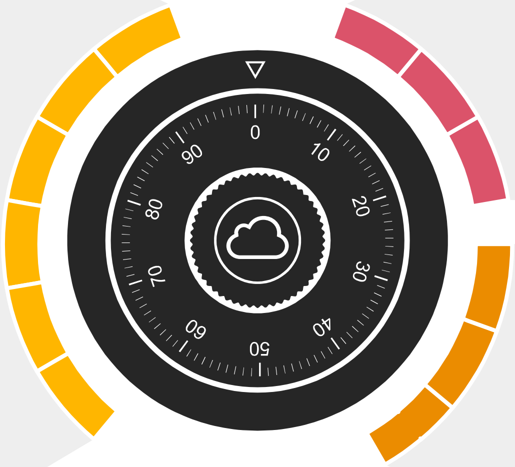
Security & Risk Management - Managing Cloud adoption risks by enhancing risk frameworks and embedding security & operational controls upfront.

Operating Model Design - Designing & implementing shared responsibility models, and establishing oversight and governance arrangements.

Contracting - Negotiating optimal pricing agreements with CSPs to maximise value from contracts & ensure commitments align with projected spending.

Data Management - Migrating data from legacy systems into the Cloud environment and establishing capabilities to govern and protect data post-migration.

AI Governance - Managing risks in Cloud-enabled GenAI applications, enhancing transparency, trust, and security to accelerate GenAI adoption.



Cyber security - Deploying effective security measures throughout the Cloud environment (including access controls, and detection and response mechanisms) to mitigate potential risks such as data loss.

Third Party Risk - Assessing and controlling risks for outsourced Cloud services, providing assurance through vendor audits and ongoing reviews.

Resilience - Guidance & contingency arrangements to manage disruption and build resilience, ensuring compliance with operational resilience regulations.

Optimisation of Cloud Expenditure - Assessing cloud expenditure and delivering cost savings through optimisation of infrastructure and services.

Sustainability - Understanding the sustainability implications of cloud usage and assisting with the journey towards Net Zero.

Process & Control Optimisation - Reducing the operational complexity associated with hybrid and/or multi-cloud environments.

Moving to the cloud ▶ **Operating in the cloud** ▶ **Optimising benefits and managing costs**

Cloud risk (continued)

Internal audit focus areas

Internal audit can provide an independent perspective on Cloud risks and the associated mitigations. Examples of key elements for internal audit to consider include:

Moving to the cloud

- Having a **clearly defined approach** to cloud transition, including assessment of the materiality of the workloads to be moved to the cloud.
- The firm's approach to relevant **regulatory notifications** (such as a material outsourcing notification) to determine whether these are comprehensive and timely.
- Understanding and enforcement of **privacy and jurisdiction** requirements, including definition of data classification and enforcement of associated controls.
- **Resilience arrangements** for the cloud transition, given the level of risk associated with the workload that is moving to the cloud.

Operating in the cloud

- **Regular cyber security risk assessments** to identify and prioritise risks, and ensure that strategies to mitigate identified risks are implemented.
- Consideration of **cyber security requirements, compliance and right to audit clauses** in contracts with CSPs.
- **Incident response plan** for cloud-related incidents.

Optimising benefits and managing costs

- **Costs are attributed accurately** to specific projects, departments, or business units, enabling better **cost accountability and management.**
- **Key performance indicators ('KPIs')** to measure the sustainability performance of cloud usage.
- Management's approach to controlling ongoing cloud costs.

Cloud compliance in UK and EU

FS firms operating in the UK and EU have an increasingly complex set of regulatory requirements to satisfy in relation to their use of cloud. Failure to adequately address these can delay cloud transitions and put overall business transformation objectives at risk.

Key considerations for firms

- **Managing concentration risk**
  The firm must be able to demonstrate to the Board and regulators that significant dependencies on Cloud Service Providers ('CSPs') and nth parties are understood and the associated concentration risk is managed.
- **Exit plans (stressed and non-stressed)**
  Comprehensive exit plans should be in place for outsourcing arrangements with CSPs, covering both stressed (e.g. failure of the service provider) and non-stressed (e.g. strategic decision) circumstances.
- **Contracting**
  The firm will need to ensure that all new cloud contracts comply with regulatory requirements, and are likely to need to remediate existing contracts to uplift these to the same standard.
- **Contingency and business**
  Contingency plans are required that demonstrate the ability of the firm to respond to and recover from failure or disruption of the cloud service without compromising the services their customers rely on.
- **Scenario testing**
  The firm must conduct regular scenario testing to assess their ability to provide services in the event of disruption to their cloud service, adjusting testing plans based on potential disruptions and new threats.
- **Mapping to business services and functions**
  The firm must be able to identify and document how their cloud services support their business functions, including identifying critical people, processes, technology, and information necessary to provide these.
- **Data security**
  The firm needs to perform due diligence on data processing jurisdictions, implement strong cloud controls for data (in-transit/in-memory/at rest), ensure data segregation in multi-tenant environments, and monitor controls provided by CSPs.
- **Threat-led penetration testing**
  The firm must incorporate threat intelligence into their penetration testing for cloud resources to ensure a 'threat-led' approach, enhancing realism and adding value to the security program.
- **Data sovereignty**
  The firm must understand and be able to control which physical jurisdictions its CSPs are storing its data in, in order to be able to demonstrate compliance with data sovereignty and reporting requirements.
- **Incident management and reporting**
  The firm must be able to comply with requirements to manage, classify and report incidents involving its cloud service consumption to relevant regulatory authorities in a timely fashion.

Internal audit focus areas

Examples of key elements for internal audit to consider include:

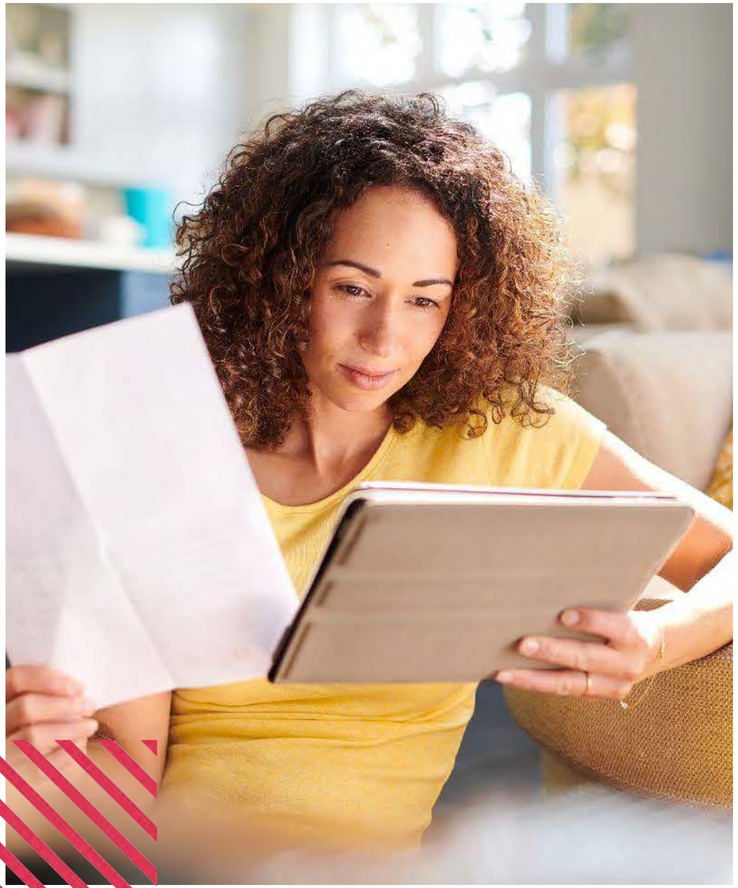
- **Vendor management:** Risk assessment and due diligence activities over CSPs, including development and testing of **exit** plans.
- **Breach notification:** Processes to comply with GDPR and other regulatory requirements for data breach notification.
- **Awareness programs:** Programs to raise awareness about **cloud** compliance and the importance of adhering to regulatory requirements.
- **Data transfer:** Mechanisms for transferring data outside the UK and EU.
- **Data processing agreements:** Data Processing Agreements ('DPAs') with CSPs and alignment with GDPR requirements (if applicable).
- **Documentation:** Documentation of cloud compliance activities, including policies, procedures, and audit reports.
- **Security configuration:** Secure configuration of cloud resources and ongoing mitigation of risks.

Data management

In a highly regulated and complex environment, organisations need to be focused on the data they have, manage and protect it appropriately, recognise the value it presents as an asset, and be able to generate real benefit from it, safely and without breaching the trust of their customers, users and employees.

Key considerations for firms

- **Data is a key business enabler** but the volume of data existing or potentially captured **presents** technical, legal and regulatory challenges.
- **Organisations must prioritise** the data within their organisations that really matters; **they** must focus on data that can be converted to new opportunities, deliver value and support risk management.
- **Data risk management** is increasingly critical in FS. As firms tackle **legacy** and new technologies, they must ensure data privacy and ethical integrity, while navigating the complexities of data sovereignty and international compliance.
- **Data ethics and monetisation:** Balancing data monetisation with ethical considerations is key in FS. UK institutions must be transparent about data usage, obtain explicit customer consent, and provide mechanisms for customers to control **their** data, ensuring ethical and responsible data practices. This is increasingly relevant as organisations look to harness new technologies such as GenAI which depend on rich datasets to have value.
- **Data is also at the forefront of the regulatory agenda** and firms need to understand the **implications** on their organisation.
  - Recent regulatory interventions, such as those by the **Federal Reserve Board ('FRB')**, underscore the importance of robust data governance. Firms have faced significant financial penalties and enhanced oversight due to deficiencies in their data management practices, highlighting the necessity for continuous improvement.
  - In addition, UK financial service firms face a rising bar of supervisory expectations as the principles of regulations such as **BCBS 239** (Basel Principles for Risk Data Aggregation and Risk Reporting) are now considered an enterprise-wide requirement above and beyond their original scope.
  - UK FS organisations must comply with the UK General Data Protection Regulation (**UK GDPR**) and other local regulations such as the Data Protection Act 2018.
  - Following Brexit, the UK has established its own **data protection framework** separate from the EU. Financial institutions need to ensure compliance with the UK's data transfer rules, including implementing **Standard Contractual Clauses ('SCCs')** and ensuring adequate safeguards for **data transferred to and from the UK.**



Data management (continued)

Key challenges in realising the power of data include:

- **Data transformation:** This is a multi-year journey requiring consistent leadership and authority.
- **Data topology:** Understanding where data is and what is important is essential for extracting its value, but this remains a challenge for organisations of all sizes.
- **Rapid technological evolution:** Significant investment is needed to meet increasing demand and expectations.
- **Talent acquisition:** Recruiting talent, particularly in emerging technologies, is increasingly competitive.
- **ESG reporting:** Measuring financed emissions is crucial for managing financial institutions' carbon footprint and aligning with net-zero commitments. Challenges include data availability and quality. Firms should consider factors like client coverage, accuracy, consistency, timeliness, relationships, costs, and trusted sources when sourcing and selecting data providers.

Internal audit focus areas

Examples of key elements for internal audit to consider include:

- **Data strategy and operating model:** Determine whether there's a clear data strategy in place to set the direction of data capabilities, in consideration of business objectives. Consider whether the operating model includes individuals with sufficient skills and experience to achieve strategic objectives.
- **Data management framework:** Assess whether a **data management framework** has been defined to set out management's principles and approach to govern data. The framework should consider relevant regulatory requirements and clearly outline key **roles and responsibilities** relating to data, including interaction with inter-related areas, such as cyber, operational resilience, and compliance.
- **Data governance:** Assess the effectiveness of governance mechanisms to oversee management of data risks, data quality issues, and any uplift required in data capabilities to meet business and regulatory requirements. Establishing training and awareness activities should also be considered to drive a **data-driven culture** and consistent good practices.
- **Data risk management:** Determine whether data risks have been identified and a risk appetite has been defined. This should support decision making and prioritisation of investment and remediation activities in data capabilities.
- **Data quality:** Ensuring accurate, consistent, and reliable data is critical for risk management, compliance, and customer service in the financial sector. Data quality standards, metrics and monitoring should be considered to ensure data integrity and support regulatory compliance and informed decision-making.

Digital identity wallets

Digital Identity provides a trust layer to online transactions, enabling entities (individuals, businesses, devices etc.) to establish the authenticity of the counterparty they are engaging with online and establish confidence in the transaction. The existence of multiple identity credentials issued by multiple issuing parties can make managing credentials challenging. To mitigate this challenge, Digital Identity Wallets can be leveraged by entities to effectively store and manage their Digital Identities. Types of Digital Identity Wallets include mobile, desktop and web applications.

Key benefits and use cases

Improve customer experience

Lower operational costs

Mitigate risk and reduce fraud

Create new revenue streams

Create deeper customer relationships

Use cases

- Improve customer trust by automating complex identity verification processes:
  - A digital identity app that allows users to securely verify their identity and share personal details with businesses and individuals through a secure online platform.
  - A platform used to simplify digital onboarding and KYC, leading to increased online sales and advisory services.
- Expand presence in the value chain to access management for FS customers:
  - Creation of accounts for banking and insurance products.
  - Single sign on for access to online and mobile banking.
  - Authorisation of high value payments.
- Launch more sophisticated use cases:
  - Retail - embedded finance in online shopping.
  - In Denmark, a product of a unique partnership between the public sector and the banking sector, is being used for online banking, mobile banking or logging into public self-service solutions.
  - In Norway, a programme used by customers for secure electronic proof of identity to create a personal electronic signature.
- Offer federated identity management services:
  - Enabling users to login to multiple banks and third parties through federated identities.
  - Offer single sign on across multiple banks and sectors.

Key considerations for firms

- **Fragmented identity management** may occur as **relying parties** do not have established mechanisms (e.g., secure Application Programming Interface or APIs) for efficient and secure digital data sharing and reception. Therefore, a system that works seamlessly with existing Digital Identity frameworks and is **interoperable across platforms** and services must be created, however this will require significant tech investment.
- The Digital Identity space is evolving, and **regulations may change** requiring organisations to navigate complex legal settings and compliance with GDPR. It is important for organisations to invest in a team that tracks this and manages the products associated with this capability.
- **Phishing and social engineering** could be used to gain access to these Digital Identity Wallets and could therefore increase the risk of identity theft, however strong authentication on the application storing these wallets and educating customers can mitigate this.
- **Not all age groups or socio-economic backgrounds have a smartphone** or access to a device where these identities will be stored, therefore alternative mechanisms should be identified while defining the processes.
- **User adoption may be low** as they will be unfamiliar with the process therefore **building user trust and confidence** regarding reliability and security of Digital Identities is crucial to expanding users and scheme participation, which may take time to establish.
- **Issuing parties** may be liable or accountable in the event of fraud or data breach, therefore clearly defined liability/accountability clauses must be outlined in contracts.

Digital identity wallets (continued)

Internal audit focus areas

- **Security measures**
  - **Encryption**: Evaluate the encryption standards used for storing and transmitting digital identities within the digital wallet.
  - **Authentication**: Assess the strength and effectiveness of authentication methods (e.g., biometrics, multi-factor authentication) used to access the digital wallet.
  - **Access controls**: Review access control policies to ensure only authorised personnel can access sensitive information.
- **Compliance and regulatory requirements**
  - **KYC and AML**: Ensure that the digital wallet complies with Know Your Customer (‘KYC’) and Anti-Money Laundering (‘AML’) regulations.
  - **Data Protection**: Verify compliance with data protection regulations such as GDPR, ensuring that personal data is handled and stored appropriately.
- **Identity verification processes**
  - **Verification methods**: Assess the methods used for identity verification to ensure they are robust and effective in preventing fraud.
  - **Accuracy and reliability**: Check the accuracy and reliability of identity verification processes to avoid false positives and negatives.
- **Operational efficiency**
  - **Process automation**: Evaluate the extent to which identity verification and onboarding processes are automated, and assess the impact on operational efficiency.
  - **Error handling**: Review mechanisms in place for handling errors and exceptions during the identity verification process.
- **User experience and accessibility**
  - **User interface**: Assess the usability and accessibility of the digital wallet across different platforms (mobile, desktop, web).
  - **Customer support**: Ensure that adequate customer support is available to assist users with issues related to the digital wallet.
- **Interoperability and integration**
  - **System integration**: Review how well the digital wallet integrates with existing systems, such as banking platforms and public service portals.
  - **Federated Identity Management**: Assess the implementation of federated identity management services and single sign-on capabilities across multiple banks and sectors.
- **Risk management**
  - **Fraud detection**: Evaluate the effectiveness of fraud detection mechanisms in place within the digital wallet.
  - **Incident response**: Review the incident response plan for handling security breaches or fraudulent activities.
- **Data quality and integrity**
  - **Data accuracy**: Ensure that the data stored within the digital wallet is accurate and up-to-date.
  - **Data integrity**: Assess measures in place to protect the integrity of data against unauthorised modifications.
- **Third-party management**
  - **Vendor assessment**: Review the security and compliance posture of third-party vendors involved in the digital wallet ecosystem.
  - **Service level agreements**: Ensure that service level agreements (‘SLAs’) with third-party vendors include provisions for security and compliance.
- **Scalability and performance**
  - **System performance**: Assess the performance and scalability of the digital wallet to handle a growing number of users and transactions.
  - **Load testing**: Review results from load testing to ensure the system can handle peak usage without degradation in performance.
- **User privacy**
  - **Data minimization**: Verify that the digital wallet collects only the necessary information required for identity verification and transactions.
  - **User Consent**: Ensure that users have given explicit consent for the collection and use of their personal data.
- **Audit trail and monitoring**
  - **Logging and monitoring**: Ensure that comprehensive logging and monitoring mechanisms are in place to track access and changes to digital identities.
  - **Audit trails**: Review audit trails to ensure that they are complete, accurate, and tamper-proof.

Artificial intelligence

Artificial Intelligence (‘AI’) presents a transformative strategic opportunity, enabling organisations to enhance efficiency, innovation and customer experience to produce a competitive advantage. However AI also introduces unique and complex risks requiring proactive assurance and oversight. As AI becomes more sophisticated, assurance functions must adapt their capabilities to ensure appropriate controls and guardrails over the development, deployment and performance of AI solutions. It is also important to ensure that the use of AI is aligned with the firm’s strategic objectives, ethical principles, regulatory obligations and stakeholder expectations.

Key industry trends

Gen AI development

AI is already growing productivity and driving efficiency across firms, with Gen AI leading the way. 70% of CEOs said GenAI will significantly change their business in the next 3 years[1]. CEOs are focusing on scaling GenAI quickly, enabling new business models and investing in the necessary skills and technologies to capitalise on the strategic opportunity.

AI regulation

With the EU AI Act entering into force on 1 August 2024, it’s broad scope, statutory requirements and focus on fundamental rights are changing the way firms classify and govern AI. Many use cases of AI emerging in the FS sector have additional governance requirements imposed.

The Act also requires organisation to comply with existing financial regulation for their AI systems, which already impose stringent requirements on risk management, performance of systems and monitoring obligations.

Responsible AI

Use of AI within firms introduces ethical challenges and AI-related incidents attract negative media coverage and highlight public concern.

Ensuring the safe and responsible scaling of AI is essential to unlocking and protecting value from the use of AI.

Accountability

The Senior Managers and Certification Regime (‘SM&CR’) stresses senior management's accountability, including AI use. The Bank of England is considering 'reasonable steps' for managers to ensure model outputs are explainable and reasonable.

PwC 27th Annual Global CEO Survey 2024

Risks and challenges

While enabling new opportunities, the ever-growing capabilities and impact of AI introduces and exacerbates a number of risks that need to be managed.

Potential threats and risks

Transparency

A lack of transparency around how and when AI is used can lead to lack of accountability and customer mistrust.

Misinformation

Most GenAI solutions are unaware and will exclude events, cases or developments that post-date its training data.

Data protection and security

Data leakage risks can be heightened due to AI tools are granted inappropriate access.

Hallucination

AI models could ‘make up’ information which is plausible but incorrect.

Discrimination

Discrimination based on protected characteristics may lead to financial exclusion.

Cyber security

AI could introduce new threat vectors, such as prompt injection attacks.

Copyright and intellectual property

GenAI models which are trained on copyright data and may pose liability risks.

Accountability

Adoption of AI models may pose accountability issues due to the lack of defined roles and responsibilities.

Misuse

GenAI could be used for malicious purposes, which could result in misalignment against the intended/approved purposes.

Artificial intelligence (continued)

Internal audit considerations

Examples of key elements for internal audit to consider include:

EU AI Act Readiness (see page 70 for more information on the Act)

On the page 71, we set out the key elements to consider in assessing AI readiness. Using this as a basis, many IA teams are working now to:

- Assess the existence and suitability of the organisation-wide AI inventory and classification of AI models as per EU AI Act requirements.
- Assess plans and progress with Implementation of necessary governance (determined by the risk classifications) covering: transparency, technical documentation, impact assessments and codes of conduct depending on the use case.
- Ensure alignment with other sectoral regulation. The risks posed by AI my fall under the scope of other regulation, such as breaches/disruption of critical AI-enabled services leading to regulatory fines.

AI risk and controls

- Understand the AI universe including use cases and development status.
- Understand your organisation's AI strategy, risk assessment, governance and policy arrangements and how they are being developed and embedded.
- Build and execute a risk-based AI audit programme (referencing materials such as the PwC AI Readiness Framework or Responsible AI Framework). Prepare tailored audit programmes for higher risk AI models.

AI-enabled Internal Audit

- Identify use cases that will drive efficiencies, optimise, automatre or enhance internal audit processes.
- Collaborate with AI steering committees and/or responsible AI council to ensure that controls and assurance remain high on the agenda
- Develop or secure access to digital skills to provide confidence in internal audit's capacity and capability to use AI effectively and provide assurance over the key and emerging risks associated with AI.

On page 74, we provide more details on use cases of AI to transform internal audit functions.

Artificial intelligence – EU AI Act

The EU AI Act is a new legislative framework that sets the precedent for AI regulation. The framework categorises AI into different risk categories and imposes obligations on users, deployers and providers of AI. Compliance timelines have been established, with the potential for significant fines for non-compliance. Effective audit of EU AI Act readiness ensures firms are aligned with the regulation in order to gain a first mover advantage and avoid legal risks.

Overview of the EU AI act

- **Risk-based classification**
  AI systems must be classified into different risk categories to support effective governance while promoting innovation. See diagram on next page.
- **Safety and fundamental human rights**
  AI systems must ensure the safety and protection of fundamental human rights, including non-discrimination, privacy, and data protection for all individuals.
- **Unified regulatory framework**
  The Act creates consistent standards in order to facilitate lawful, safe, and trustworthy AI in the EU Single Market.
- **Broad, extraterritorial impact**
  The AI Act applies to AI systems across all sectors and all systems operating in the EU, or with an impact in the EU, even if the system is abroad. UK firms are impacted if they procure, use or deploy systems on the EU market or impact EU customers.
- **Across the AI value chain**
  Most obligations fall on providers (creators) and deployers (users), but importers and distributors are also affected.

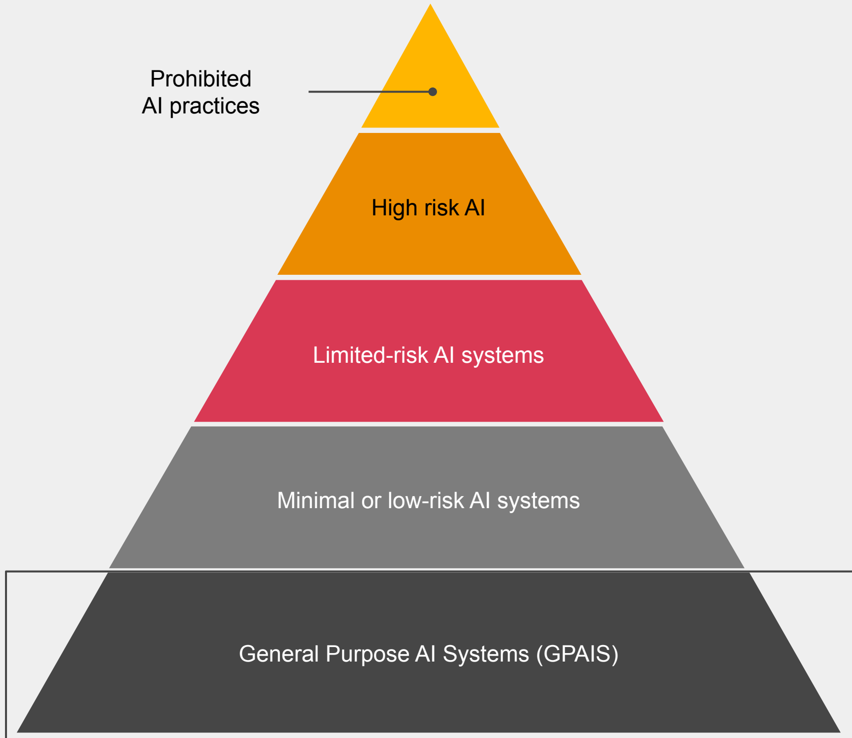
Compliance timelines

Starting point

- **December '23** EU AI act agreed.
- **01 August 2024**
- **+6 months prohibitions** on unacceptable risk shall enter into force.
- **+12 months** obligations on providers of GenAI models go into effect.
- **+18 months** Commission implementing act on **post-market monitoring obligations.**
- **+24 months** obligations on High-risk AI systems, as defined in Annex III systems, go into effect.
- **+36 months** obligations related to high risk AI systems subject to product safety regulation becomes applicable.
- **2030** AI components of large-scale EU IT systems in Freedom, Security, and Justice must comply.

Artificial intelligence – EU AI Act (continued)

How are AI systems classified, according to the EU AI Act?



AI systems that are outright banned due to potential to cause significant harm.

E.g. Through manipulative techniques that impairs decision making through exploiting vulnerabilities (such as age, physical or mental disability).

AI systems that cause risk or harm on people´s health, safety and fundamental rights. These are subject to stringent regulatory requirements.

E.g. systems for evaluating credit worthiness or pricing in life and health insurance.

AI systems that pose lower levels of risk, and as such as subject to lighter regulatory requirements.

E.g. chatbots, emotion recognition systems or deep fakes.

AI systems that do not pose significant risks and do not require regulatory oversight (however must comply with existing legislation).

E.g. Spam filters and video games.

AI systems that display significant generality, performing a wide range of distinct tasks. These are further classified into risk tiers and are subject to transparency and documentation requirements.

General purpose models are regulated separately, which covers the following:

Tier 1: All General Purpose AI (GPAI)

Tier 2: High impact and system risk

- **Transparency obligations,** including statement about the training data used.
- **EU copyright policy.**
- Performance of **model evaluation, including adversarial testing** to assess and mitigate possible systemic risk.
- **Serious incident** monitoring and reporting.
- **Energy consumption** monitoring and reporting.

Company fines for violations of the act[1] range from…

€35m or **7%**
of global annual turnover (if higher)
– **for violations of banned AI**

€15m or **3%**
of global annual turnover (if higher)
– **for violations of other obligations**

€7.5m or **1%**
of global annual turnover (if higher)
– **for supplying incorrect information**

[1]EU AI act: Article 99 – penalty.

Artificial intelligence – AI readiness framework

Navigating the evolving landscape of AI involves careful consideration of the different domains that comprise effective and responsible operationalisation of AI at scale.

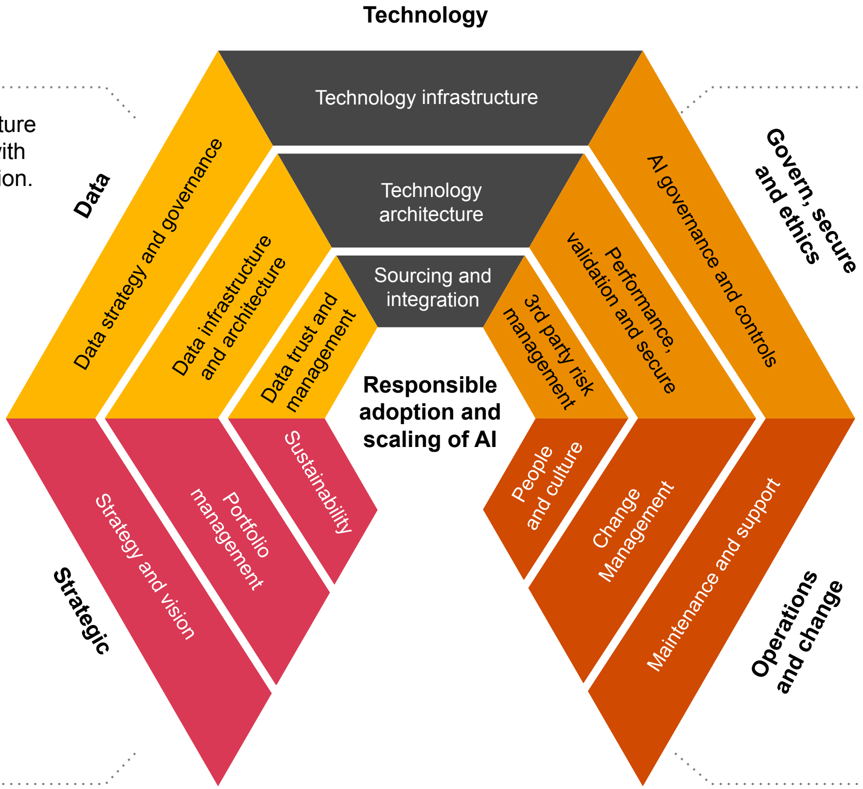
PwC's AI readiness framework

Navigating the evolving landscape of AI involves careful consideration of the different domains that comprise effective and responsible operationalisation of AI at scale. The AI readiness domains, developed by PwC and illustrated on the right, are aligned with industry standards and regulation such as the National Institute of Standards and Technology ('NIST') AI Risk Management Framework and the EU AI Act.

Evaluates the infrastructure, tools, and technical capabilities to determine the firm's preparedness for AI adoption.

Examines the quality, accessibility,infrastructure and governance of data, ensuring it aligns with the firm's needs for effective AI implementation.

An approach based on Responsible AI ensures firms use of AI is ethical, fair, and transparent, and in line with legal and societal expectations.



Alignment of the AI initiative against the firm's strategic objectives, with ESG considerations built into the strategy to ensure sustainable adoption.

Assesses the organisational readiness for AI by evaluating the alignment of workforce skills, attitudes, and collaboration with AI technologies to foster a supportive and adaptable cultural environment.

Artificial intelligence – AI readiness framework (continued)

Internal audit focus areas

Examples of key elements to consider in assessing AI readiness are:

Domain	Key Considerations
Strategic	• AI strategy to ensure clear ownership, long-term viability, alignment to corporate goals, and effective communication across the organisation. • Robust framework for managing AI opportunities, from identification and communication to monitoring, review, and realisation. • Capability to measure AI initiatives against ESG goals, assess environmental implications, and optimise costs through Financial Operations ('FinOps') principles.
Data	• Data governance framework to ensure consideration of regulatory compliance, data reliability, and trust in AI systems. • Data infrastructure to ensure AI integration and effective data management. • High data quality and effective management of personal data.
Technology	• Effective processes and mechanisms for sourcing new AI solutions and integrating them into the existing tech landscape. • Standardised AI development lifecycle, maintaining code quality and software integrity in alignment with industry standards. • Robust technology infrastructure, architecture, and cloud resources, adequately set up to support the development and deployment of AI solutions.
Governance, Security and ethics	• Governance in place to manage AI risks, including relevant standards, policies and guidelines, complying with best practices from regulators and standard-setters. • AI assurance solutions including comprehensive testing, explainability, secure design, bias detection, and user experience validation. • Assessment and management of potential risks and vulnerabilities from third parties, ensuring adherence to business policies and contractual requirements.
Operations and change	• AI-driven cultural transformation and training efforts to promote organisation-wide change and to leverage AI capabilities. • Comprehensive change management practices addressing cultural, technological, and business implications, ensuring business processes adapt to AI changes and planning for long-term viability. • Appropriate resources and mechanisms are in place to manage, maintain, and support AI solutions post-deployment.

Transforming Internal Audit with Artificial Intelligence

AI has the potential to revolutionise Internal audit functions - transforming capabilities, providing opportunities for optimisation of resources and better insight gathering through more detailed analysis. Here are some examples and key benefits of AI use cases that are changing the way organisations conduct internal audit:

01

AI enabled control testing

The capability of AI to process large volumes of unstructured data can be leveraged in controls evaluation and testing to recognise patterns and propose findings. AI is capable of:

- Reviewing documents, emails and summarising evidence submitted.
- Identifying gaps in data.
- Generating test scripts for remediation of identified issues.
- Evaluating large control databases to identify duplicate controls and incomplete controls description.

02

GenAI internal audit planning and support

GenAI models can help design internal audit plans and provide support on audit engagements, drawing from internal audit methodologies, web searches for relevant risk assessments and historic annual reports. Use cases include:

- Automating risk assessments.
- Developing audit plans with tailored domains and risk theming.
- Drafting audit scope and announcement memorandums (or Terms of Reference) to auditees.

03

AI enabled stakeholder engagement

GenAI solutions can enable more effective stakeholder engagement using tools such as Microsoft Copilot, which can improve productivity through:

- Drafting relevant stakeholder questions and meeting agendas.
- Transcribing meetings and generating summaries.
- Identifying next steps based on stakeholder conversations.

04

Continuous monitoring

AI tools can be used to continuously monitor systems and processes to automatically flag risks and provide an audit trail for review. Examples of continuous monitoring include:

- Identifying of anomalies and fraudulent transactions.
- Automating compliance monitoring to ensure compliance with policies and regulation.
- Embedding predictive analytics for forecasts and ongoing risk assessments.

05

Audit practice and quality assurance support

AI can significantly enhance audit quality assurance and enable cost efficiency. Some examples are:

- Using GenAI to review audit reports and completed files to identify quality-related issues.
- Incorporating interactive chatbots and virtual assistance to provide real time support to auditors on methodologies and audit standards.

Key benefits:

01	02	03	04	05
Reduce human error in data analysis and reporting	Improve accuracy of data analysis and verification against regulations	Increase efficiency and cost saving through process automation	Enable ongoing monitoring and real-time risk detection	Enable ongoing quality and continuous improvement

Digital transformation

Firms continue to evolve and progress with digital transformation programmes with the goal of increasing value through innovation, invention, customer experience or efficiency. Whilst many clients are undertaking significant change activities, many are struggling with delivery risk across the course of large transformation programmes.

Key industry trends

Common challenges

Many transformation programmes have heightened risks of either failing or not delivering on time or budget. In our experience the most common root causes include:

- Weak governance.
- Poor planning.
- Insufficient change control.
- Budget and cost overruns.
- Programme risks not align to entity risk strategy.
- Poor benefits management.
- Mismatched people and culture, employee resistance to change.
- Lack of stakeholder engagement.
- Insufficient resourcing, lack of knowledge and skills.

Internal audit focus areas

When conducting an internal audits focusing on digital transformation, consider the following key areas:

Assess change management and organisational readiness

- Alignment of change initiatives with overall business goals and objectives.
- Readiness and capability of firm to adopt and sustain new technologies.

Evaluate governance and compliance

- Allocation of roles and responsibilities, and design of governance forums.
- Effectiveness, appropriateness and timeliness of the escalation and approval process by relevant committees, Senior Management Functions ('SMFs') and the Board.

Review resilience approach

- Processes to assess materiality of change including consideration of impact to Important Business Services.
- 'Failback/'what if'' scenario assessments are in place in the event the programme is delayed or stopped.
- Effectiveness of existing risk management processes to identify, assess, escalate and report key IT change management risks.
- Lessons learned process (including a prioritisation approach over identified actions) to enable continuous improvement.

Assess technology integration and interoperability

- Integration of new digital tools with existing systems.
- Interoperability and compatibility of different technologies.

Frameworks and approaches to methodically step through what can go wrong are also helpful to focus attention on and mitigate risk. See an example below.

Financial crime

Financial crime

The FCA continues to focus on financial crime risk and firm's systems and controls to mitigate this.

Financial crime

- The FCA's 2024/25 Business Plan underscores its commitment to reducing and preventing financial crime as one of its primary objectives. This focus not only aims to protect the integrity of the financial system, but also ensures the safeguarding of consumers, particularly those in vulnerable circumstances who are more susceptible to fraud. Building on previous efforts, the FCA plans to intensify its proactive assessments of firms' Anti-Money Laundering ('AML') systems and controls. Additionally, the development and application of advanced data-led analytical tools will play a crucial role in enhancing the effectiveness of AML supervisory activities.
- In alignment with its ongoing strategy, the FCA will continue to employ a data-driven approach to supervise firm's sanctions systems and controls. This comprehensive surveillance is vital for identifying and mitigating risks associated with market abuse and financial crime. By leveraging technological advancements and fostering a culture of compliance, the FCA aims to bolster the resilience of the financial sector against evolving threats.
- In September 2023, His Majesty's Treasury ('HM Treasury') extended information sharing requirements for wire transfers, known as the travel rule, to include cryptoassets. The travel rule sets the information sharing and record keeping requirements which apply to bank transfers and to transfers of cryptoassets, to assist in the prevention and detection of money laundering. The new market abuse regime for cryptoassets will be based on elements of the Market Abuse Regulation (MAR). The market abuse offences will apply to all persons committing market abuse using cryptoassets which are admitted (or requested to be admitted) to trading on a UK cryptoasset trading venue, and apply regardless of where the person is based or where the trading takes place.

For more information on global digital assets and crypto developments, please see PwC's Global Crypto Regulation 2024 Report.

Key priorities for 2025

01 **Enhanced surveillance systems:** Adoption of advanced technologies for real-time monitoring and analysis to detect and prevent market abuse.

02 **Comprehensive risk assessments:** Regular updates to AML and financial crime risk assessments to incorporate new regulatory requirements and emerging threats (see next page for further details).

03 **Governance and oversight:** Strengthening governance frameworks to ensure clear accountability and robust oversight of market abuse controls.

04 **Training and awareness:** Ongoing training programs to educate employees on market abuse risks and promote a culture of compliance.

05 **Collaborative efforts:** Continued collaboration with international regulatory bodies to share best practices and enhance the global market abuse detection framework.

Financial crime (continued)

Comprehensive risk assessments

The FCA has frequently communicated that firms approach to risk assessment is not satisfactory. A risk assessment forms the basis of a firm's risk based approach and is therefore a key consideration for internal audit work.

Comprehensive risk assessments are critical for identifying, evaluating, and mitigating potential risks associated with financial crime, including market abuse, money laundering, and terrorist financing. These assessments enable firms to understand their risk exposure and implement effective controls to mitigate those risks.

Key components of risk assessments

Identification of risk factors:

- Assessing the risk profiles of customers, including factors such as geographical location, industry, and transaction behaviour.
- Evaluating the inherent risks associated with specific products or services offered by the firm.
- Identifying high-risk jurisdictions that are prone to financial crime activities.

Data collection and analysis:

- Utilising data analytics to gather and analyse vast amounts of information related to transactions, customer behaviors, and market trends.
- Employing machine learning ('ML') models to detect anomalies and predict potential risks.

Regulatory compliance:

Ensuring that risk assessment methodologies comply with regulatory requirements, such as those outlined in the FCA's market watch publications and the EU's Market Abuse Regulation ('MAR').

Periodic reviews:

- Conducting regular reviews and updates of risk assessment methodologies to incorporate new risk factors and regulatory changes.
- Engaging in continuous improvement by learning from past incidents and adapting to emerging threats.

Financial crime (continued)

The FCA continues to focus on financial crime risk and firm's systems and controls to mitigate this.

Key considerations for firms

Enhanced surveillance systems

Implement advanced, adaptable surveillance systems for real-time monitoring and analysis to detect financial crimes. Ensure systems are updated regularly to address new trading patterns, emerging threats, and regulatory requirements to mitigate potential financial crime risks.

Comprehensive risk assessments

Regularly update risk assessments to incorporate new regulatory requirements and emerging threats. Use advanced data analytics to evaluate customer, product/service, and geographical risks, ensuring due diligence procedures are commensurate with the financial crime risks identified.

Governance and oversight

Ensure active Board and senior management involvement in overseeing risk management strategies. Define clear accountability and develop comprehensive policies for market abuse surveillance. Regularly review and enhance governance frameworks to maintain robust oversight and mitigate financial crime risks.

Training and awareness

Provide ongoing training on market abuse risks, regulatory requirements, and best practices. Promote a culture of compliance and ethical behavior to ensure employees are vigilant and proactive in identifying and mitigating risks.

Due diligence and screening

Enhance due diligence processes and regularly update sanctions screening systems. Ensure comprehensive understanding of customer identities and end-users in trade finance transactions to avoid regulatory and legal risks associated with sanctions exposure.

Regulatory coordination

Collaborate with international regulatory bodies to share insights and best practices. Ensure compliance with local and international standards to mitigate global compliance risks associated with market abuse and financial crime.

Internal audit focus areas

Policy, Procedure and control evaluation:

- Review how the firm identifies higher risk factors through the design and implementation of procedures.
- Assess detailed customer take-on processes to ensure that high-risk factors are adequately identified and managed, considering the effectiveness of current controls and their alignment with regulatory standards.

Compliance monitoring:

Conduct thorough testing of the firm's sanctions controls and screening lists used for customer verification. This should include completeness testing and sample name testing to verify screening alert outputs. Utilise tools like the FCA's customer name screening testing tool to evaluate system effectiveness and identify any gaps.

Risk assessment methodology:

- Evaluate the firm's methodology for conducting risk assessments, particularly in mitigating inherent and residual risks and verify that all applicable risk factors are considered, referencing industry guidance and national risk assessments.
- Evaluate the firm's controls for their effectiveness in addressing identified financial crime risks.

Training programmes:

- Assess whether the firm's training programmes comprehensively cover all relevant risks, including market abuse, money laundering, and terrorist financing.
- Assess whether training is effectively communicated to all employees and includes up-to-date information on regulatory changes and best practices.

Economic crime and corporate transparency act

Failure to prevent fraud offence

The UK government published a policy paper on 1 March 2024, confirming that it will require corporations to implement measures to prevent fraud, with failure to do so constituting an offence under the economic crime and corporate transparency act. The requirements will apply to all large organisations operating in the UK.

Overview of the offence

The ‘failure to prevent fraud’ offence is part of the Economic Crime and Corporate Transparency Act 2023. This new offence makes organisations criminally liable if they fail to prevent fraud committed by an employee, agent, or any associated person intended to benefit the organisation. The offence is designed to enhance corporate accountability and drive a cultural shift towards better fraud prevention.

Key dates and developments

26 October 2023: The Act received Royal Assent, officially becoming law.

Spring 2024: The UK government published detailed guidance on “reasonable procedures” for fraud prevention. This guidance is crucial for organisations to understand the necessary measures for compliance.

Late 2024 to early 2025: The “failure to prevent fraud” offence will come into force following the publication of the guidance, operationalising the new legal requirements.

Scope and applicability

- The offence applies to large organisations, defined by meeting at least two of the following criteria: more than 250 employees, over £36 million in turnover, or more than £18 million in total assets.
- It covers various fraud offences, including fraud by false representation, failing to disclose information, abuse of position, false accounting, and fraudulent trading.
- The offence has extraterritorial reach, applying even if the associated person committing the fraud is based outside the UK, provided the fraud benefits the organisation.

Reasonable procedures defence:

Organisations can avoid prosecution by demonstrating that they had reasonable procedures in place to prevent fraud. The government will provide detailed guidance on what constitutes reasonable procedures.

Penalties:

Organisations convicted under this offence can face unlimited fines. Courts will consider all circumstances to determine the appropriate fine.

Economic crime and corporate transparency act (continued)

Failure to prevent fraud offence

Key considerations for firms

- **Risk assessment:** Conduct comprehensive fraud risk assessments that cover fraud benefiting the firm, not just fraud perpetrated against it.
- **Governance and oversight:** Ensure high-level commitment to fraud prevention, including Board-level oversight and clear accountability.
- **Anti-fraud policies and training:** Develop and implement robust anti-fraud policies and provide tailored training, especially for high-risk roles within the firm.
- **Financial controls:** Reinforce financial controls to detect and investigate potential fraud, incorporating mechanisms like four-eye checks.
- **Third-party due diligence:** Integrate fraud due diligence with existing processes for third-party agents and contractual relationships.
- **Monitoring and review:** Regularly audit and review fraud prevention measures, and adapt whistleblowing procedures to include fraud reporting.

Internal audit focus areas

- **Policy and procedure evaluation:** Review existing anti-fraud policies and procedures, and confirm that they have been updated to include consideration of the requirements of the economic crime and corporate transparency act.
- **Compliance monitoring:** Assess ongoing compliance with the new requirements, including thorough documentation and evidence of reasonable procedures.
- **Training programmes:** Assess whether the firm's training programmes comprehensively cover all relevant fraud risks and whether training is effectively communicated to all employees and includes up-to-date information on the regulatory changes and best practices.
- **Ongoing assurance:** Assess processes in place to identify and respond to fraud risks promptly, ensuring a proactive stance towards fraud prevention.

European Anti Money Laundering Authority – AMLA

On 22 February 2024, it was announced that the the Anti-Money Laundering Authority ('AMLA') will be headquartered in Frankfurt, Germany, and it was confirmed that it will require financial institutions to implement enhanced due diligence (EDD) measures for high-risk transactions in all but exceptional cases. The requirements will apply to all financial institutions operating within the EU, including banks, insurance companies, and investment firms.

What is AMLA?

The AML Authority (AMLA) is a new supervisory body established by the EU to oversee and enforce laws aimed at preventing money laundering and terrorist financing across member states. It was proposed as part of the EU AML Reform Plan to address shortcomings in the current AML and Counter- Terrorist Financing (CFT) framework and enhance the coordination and effectiveness of AML efforts within the EU.

Key dates and developments

July 2021:

Proposal announcement – The European Commission proposed the establishment of AMLA as part of a broader AML reform package. This proposal aimed to address existing deficiencies in the EU's AML/CFT framework.

December 2023:

Agreement on revised draft – The revised draft of the AMLA regulation was agreed upon, setting the stage for the formal establishment and operationalisation of the authority. This draft included comprehensive details about the structure, powers, and responsibilities of AMLA.

Early 2024:

Public hearings and location selection – Joint public hearings by the European Council and Parliament were conducted to discuss and refine the AMLA framework. Frankfurt was chosen as the headquarters for the new authority.

July 2025:

AMLA regulation comes into effect – The AMLA regulation is expected to come into force in July 2025, which marks the beginning of AMLA's formal establishment and preparatory phase for direct supervisory activities.

2028:

Commencement of direct supervision – AMLA is anticipated to start its direct supervisory activities over selected high-risk entities. This will include rigorous oversight and enforcement actions aimed at ensuring compliance with AML regulations across the EU.

European Anti Money Laundering Authority – AMLA (continued)

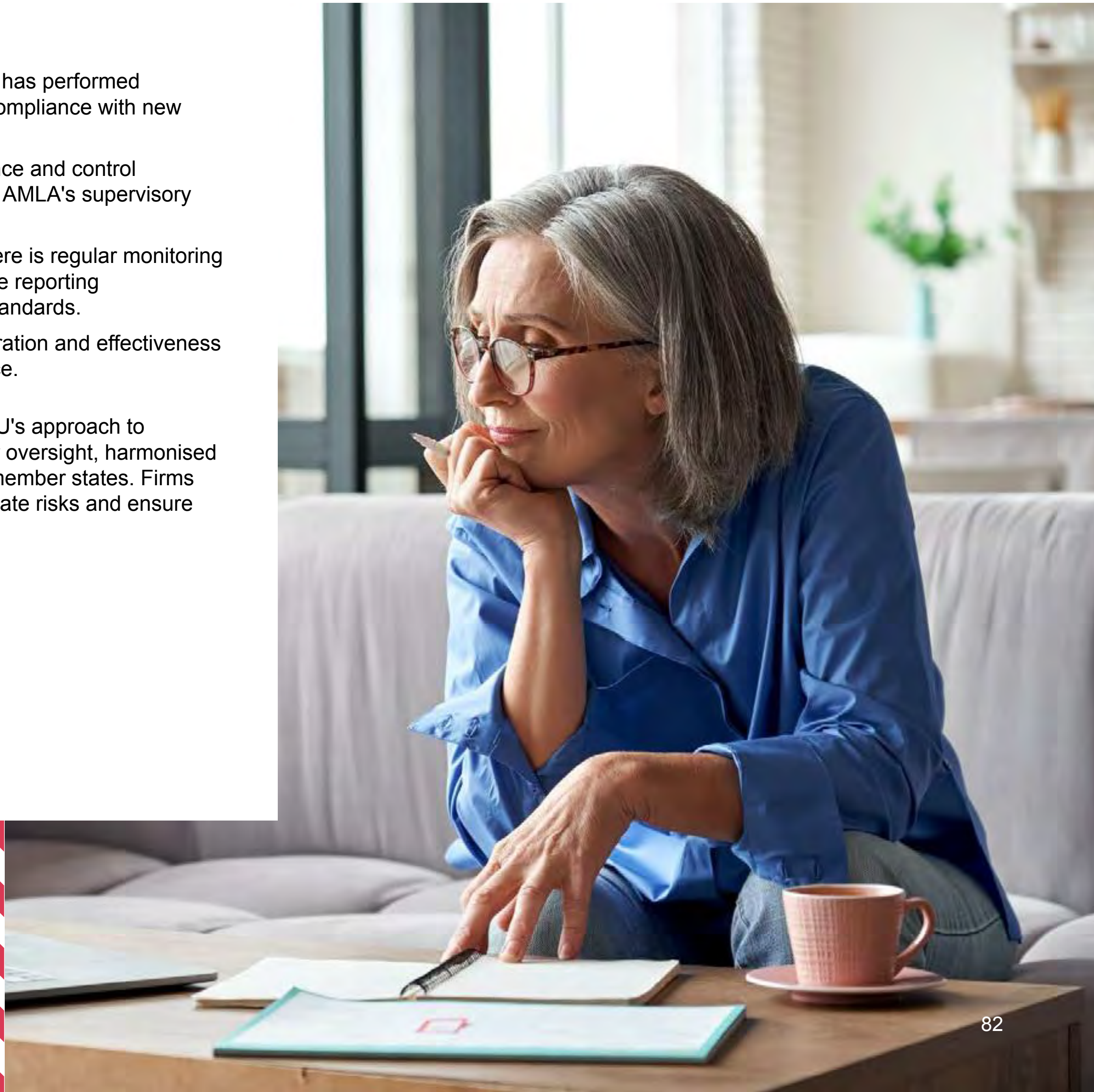
Key considerations for firms

- **Direct Supervision:** Certain high-risk entities, including cross-border financial institutions and crypto asset service providers, will come under direct supervision.
- **Enhanced Compliance Requirements:** Firms will need to adapt to new AML/CFT supervisory methodologies, including detailed rules on Customer Due Diligence (‘CDDs’), beneficial ownership, and reporting standards.
- **Technology and Automation:** There will be a need for advanced technological solutions to manage enhanced compliance checks and data accessibility.
- **Governance and Oversight:** Firms must ensure robust governance structures to facilitate compliance with AMLA regulations.
- **Training and Hiring:** Firms may require additional training and staffing to meet the new regulatory demands.

Internal audit focus areas

- **Risk Assessments:** Assess whether the firm has performed comprehensive risk assessments to ensure compliance with new AMLA requirements.
- **Governance Frameworks:** Review governance and control frameworks to assess whether they align with AMLA's supervisory approaches.
- **Compliance Monitoring:** Assess whether there is regular monitoring of compliance activities, and whether there are reporting mechanisms to ensure adherence to AMLA standards.
- **Technological Integration:** Assess the integration and effectiveness of technological tools used for AML compliance.

AMLA represents a significant evolution in the EU's approach to combating financial crime, emphasising stronger oversight, harmonised regulations, and enhanced cooperation across member states. Firms must proactively adapt to these changes to mitigate risks and ensure compliance.



Increase in financial crime section 166 reviews

The PRA and FCA have started commissioning more s166s during the previous two years, but why? There are a number of factors at play. Post the Covid pandemic, regulators now have the room to take a step back and return To business as usual (‘BAU’). The PRA and FCA are also using s166s more broadly, issuing them to financial institutions for purposes beyond pre-identified risk or whistleblowing.

Under section 166A of FSMA 2000, the PRA may require a firm to appoint, or may itself appoint, a skilled person to collect or update information.
The use of this skilled person is a supervisory tool, not a punitive tool. With this, the tool may be used:

I. For diagnostic purposes: To identify, assess and measure risk.
II. For monitoring purposes: To track the development of identified risks, wherever these arise.
III. For preventative action: To limit or reduce identified risks and so prevent them from crystallising or increasing.
IV. For remedial action: To allow the PRA to respond to risks when they have crystallised.

These powers can be used when the FCA or PRA has concerns regarding a firm’s risk framework and/or the effectiveness of its systems and controls, considering it necessary to obtain expert analysis and recommendations for areas of improvement and remedial actions which follow.

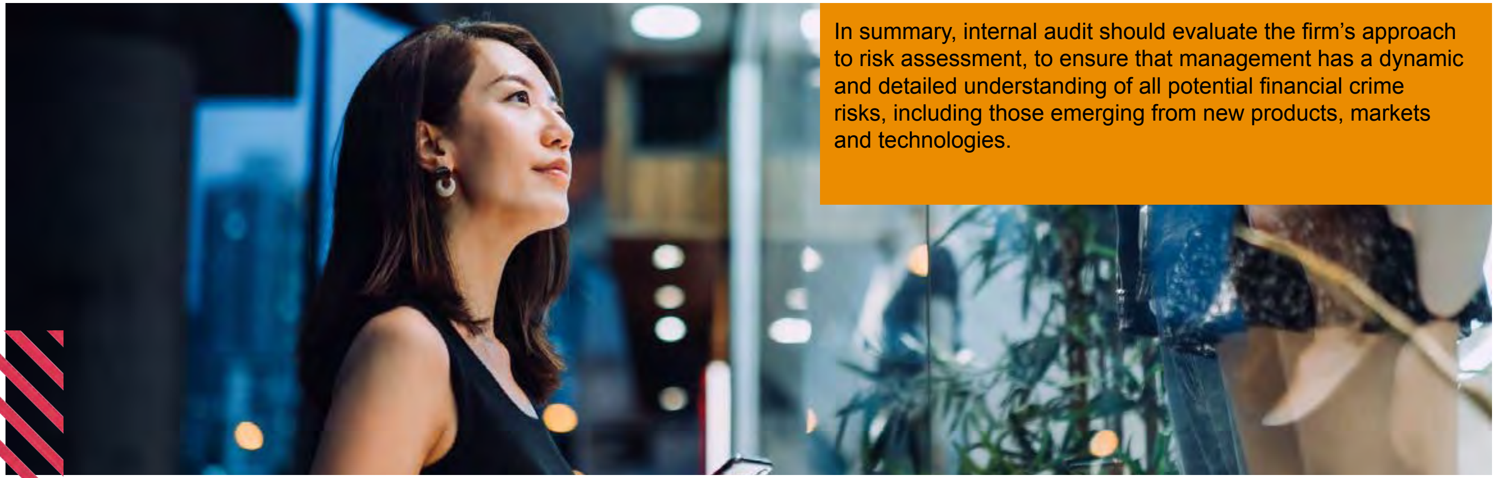
Increase in financial crime section 166 reviews (continued)

Key considerations for firms

- **Robust risk management framework:** This includes a comprehensive risk assessment that identifies and evaluates potential financial crimes, alongside clear policies and procedures designed to mitigate these risks. The framework should ensure ongoing monitoring and reporting, underpinned by effective internal controls and technology stacks.
- **Governance, compliance and training:** Strong governance structures and oversight by senior management are essential. This area also covers adherence to all relevant laws and regulations, including AML, sanctions, and anti-bribery measures. Additionally, regular and specialised training for staff is crucial to maintain high levels of awareness and compliance.
- **Evaluation and continuous improvement:** Regular independent testing and audits should be conducted to assess the effectiveness of financial crime controls. Firms must also demonstrate that any past deficiencies have been addressed through effective remediation, and they also need to manage risks associated with third parties and affiliates effectively.

Internal audit focus areas

- **Policy implementation and enforcement:** Assess whether the firm has policies designed to mitigate identified risks and that these are effectively communicated and enforced, and are aligned with regulatory requirements. This includes evaluation of policy adherence across all levels of the firm.
- **Control effectiveness and technology integration:** Assess the effectiveness of control measures, including transaction monitoring systems, CDD processes, and compliance protocols. In addition, assess the effectiveness of the integration and performance of tech solutions used to detect and prevent financial crime.
- **Regulatory compliance and reporting:** Review compliance with all applicable financial crime regulations and reporting requirements. Evaluate how management stays updated with changes in legislation and assess the firm's responsiveness to regulatory advice and directives.
- **Training, culture and remediation measures:** Assess whether the firm's training programmes comprehensively cover all relevant risks, including financial crime risks. Assess the effectiveness of training programmes in increasing staff awareness and understanding of financial crime risks. Additionally, evaluate the culture of compliance within the firm and the success or remediation measures taken to address previous audit failings.
- **Response responsibility:** By identifying and addressing issues through their findings, this proactive approach by internal audit should support effective management of regulatory supervision and therefore reduce the risk of regulatory sanctions and interventions including s166 reviews. Where external reviews are to be conducted, internal audit teams should be equipped to review low-risk files effectively.



In summary, internal audit should evaluate the firm's approach to risk assessment, to ensure that management has a dynamic and detailed understanding of all potential financial crime risks, including those emerging from new products, markets and technologies.

Global elections and PEPs

With elections taking place across the globe, it is no surprise that there will be significant fluctuation in who would be considered to be Politically Exposed Persons ('PEPs') across many international jurisdictions. Financial institutions will begin to feel the mounting pressures on teams and resources to enforce risk appetites.

Overview

- Politically exposed persons ('PEPs') are individuals with prominent public functions, such as heads of state, senior politicians, judicial or military officials and executives of state-owned enterprises, who pose higher risks for involvement in bribery and corruption.
- Global elections in 2024-25 will result in movement in the number of PEPs, significantly impacting the compliance and risk management strategies of financial institutions.

Significant dates and developments

- **Late 2024:** Major elections in key regions including the United States, India and the EU will introduce new PEPs and elevate regulatory scrutiny.
- **2025:** Continuation of election cycles, particularly in emerging markets, will further expand the PEP landscape, necessitating ongoing adjustments to risk management practices.

Global elections and PEPs (continued)

Key considerations for firms

- **Resourcing and planning:** Allocate sufficient resource to enhance due diligence (‘EDD’) processes, ensuring comprehensive identification and management of new PEPs. Develop strategic plans to address the influx of PEPs and adjust risk assessments accordingly.
- **Risk Appetite and Exiting PEPs:** Regularly review and update the firm’s risk appetite concerning PEPs. Establish clear procedures for exiting relationships with PEPs who prose excessive risks, aligning with the firm’s risk appetite.
- **Enhances Screening Processes:** Employ advanced technologies like AI and machine learning (‘ML’) for efficient PEP screening, be that in-house or outsourced. When outsourcing, ensure sufficient governance and oversight is in place.

Internal audit focus areas

Policy and procedure evaluation

- **Effectiveness assessments:** Assess the effectiveness of policies and procedures related to PEP identification and management.
- **Regulatory alignment:** Review policies to ensure that they align with current regulatory expectations, sanctions watch lists and best practices.

Compliance monitoring

- **Control testing:** Conduct thorough testing of compliance controls, including EDD and ongoing monitoring of PEPs.
- **Analytical tools:** Assess whether the firm uses advanced analytics and tools to enhance the effectiveness of monitoring systems, and whether these are operating effectively.

Risk assessment methodology

- **Evaluation**: Evaluate the firm’s risk assessment processes, focusing on mitigating risks associated with new PEPs.
- **Comprehensive inclusion:** Assess whether risk assessments incorporate all relevant factors and regulatory requirements.

Incident response and reporting

- **Response procedures:** Review the firm’s procedures for responding to potential sanctions violations.
- **Reporting process:** Verify that the firm has a clear process for reporting violations to regulatory bodies, and understood by all relevant employees.

Fraud risk management

A financial, reputational and regulatory risk – fraud is a critical pain point for all financial institutions.

Financial Institutions' role at the centre of economic activity means they are uniquely exposed to fraud risk. As well as managing typical corporate fraud risks (e.g. internal fraud, supplier fraud, etc.) they are exposed to risks of customer fraud and have regulatory and commercial imperatives to manage fraud threats impacting their customers.

Headline rates of fraud are rising and new threat types are constantly emerging as criminals seeks to take advantage of both system and human vulnerabilities. Financial Institutions must constantly evolve their counter-fraud capabilities to maintain effective risk management in a highly dynamic threat environment.

This need to constantly invest and improve counter-fraud capabilities drives significant spend by Financial Institutions. The regulation on obligations to reimburse customer fraud losses will come into effect on 7 October 2024, adding further cost overheads. Financial Institutions must ensure their investment in controls is effective against this increased financial risk.

Key considerations for firms

- **Mutating fraud threats demand constant investment**

  Firms must manage constantly evolving threats driven by changing customer behaviours, new products and emerging technologies.
- **Economic pressure incentivising fraudsters**

  Cost of living pressures are driving increases in fraud attacks and in money mule activity.
- **Rising political pressure will increase scrutiny**

  The Economic Crime Plan and Fraud Strategy have set high ambitions for fraud reduction, with banks and payment firms at the centre of the response.
- **New regulatory requirements**

  New obligations to reimburse victims of fraud, alongside the Consumer Duty will require investment to achieve compliance.
- **Imperative to maintain trust and reputation**

  Transparency around fraud rates and ease of account switching means effective counter-fraud capabilities is a commercial imperative.
- **Balancing commercial exposures**

  Robustness of control, customer experience and efficiency are finely balanced.

Fraud risk management (continued)

Internal audit focus areas

01

Governance: Assess whether the firm has defined its fraud strategy and risk appetite and evaluate its approach to monitoring control effectiveness to facilitate continuous improvement.

02

Risk assessments: Evaluate the firm's approach to understanding how fraud risk may arise across the business, recognising that threats will change as fraudsters develop new techniques and as a business evolves.

03

Policies and procedures: Assess whether the policies and processes used to monitor, identify and escalate fraud risk are effective and fit for purpose in the context of risks arising from changes in the business and are appropriately documented.

04

Resources and organisational structure: Assess whether the firm has the right resources with the right skills that are available to deliver effective fraud risk management and that roles and responsibilities are clearly understood.

05

Systems and controls: Assess whether the firm has Implemented appropriate controls in areas of likely fraud risk and verify that these controls have been calibrated based on the defined fraud risk appetite.

06

Data, reporting and analytics: Evaluate the effectiveness of the firm's approach to providing information and insight to support good decision making, in particular to understand whether fraud is being managed within a defined risk appetite. Assess whether capabilities to identify, monitor and measure fraud risk and fraud losses have been developed and implemented.

07

Training: Review and assess management's approach to training and development to ensure staff remain competent to effectively manage fraud risk.

08

Continuous improvement and change management: Evaluate the firm's approach to monitoring ongoing effectiveness of all elements of fraud risk management, ensuring that fraud strategy and underlying processes remain effective and up to date.

Environment, Social and Governance ('ESG')

Environment, Social and Governance (ESG) overview

The regulatory environment across ESG is constantly maturing, with new initiatives emerging. Firms need to have a clear strategy for managing risks and opportunities that arise from these market and regulatory pressures. Second and third lines are proactively engaging with ESG topics – particularly in larger organisations which are already subject to a range of regulatory requirements and may have made public sustainability commitments.

ESG concerns are shaping organisations by influencing their strategy, governance, and culture, and impacting all of their functions.

Firms need to consider ESG risks across their functions, make new disclosures, and play a more active role in driving sustainable outcomes for investors, society and other key stakeholders. FS regulators are also focusing on financial risks arising from climate change. Therefore, firms need to ramp up capabilities and embed climate risks in their business strategy, decision-making processes, and financial reporting.

At the same time, ESG provides commercial and transformative opportunities (e.g gaining competitive advantage, attracting investors, efficiency in operations etc) for firms to seize in order to drive change.

Please also refer to our ESG website for further information.

Key themes across ESG

Environmental concerns
The impact of a firm on the environment and the impact of climate change on a firm's operations and sustainability.

Social concerns
The impact of a firm on individual and societal wellbeing.

Governance concerns
The processes a firm has for decision making, reporting, and ethical behaviour.

Environment, Social and Governance (ESG) overview (continued)

The key themes across the three aspects of ESG are highlighted below. On the following pages, we will delve into these key themes in more detail, providing further guidance on the role that internal audit can play.

The "E" in ESG: Net Zero – The UK Government in 2021 set out greening finance: a roadmap to sustainable investing, setting out its green finance agenda, which includes making transition plan disclosure the norm across the UK, and the UK Transition Plan Taskforce ('TPT') was subsequently established to help firms develop 'gold standard' climate transition plans.

The "E" in ESG: Greenwashing and labels –The FCA introduced an Anti-Greenwashing rule for all FCA-authorised firms, intended to ensure all sustainability-related claims in relation to products and services are 'fair, clear, and not misleading'. The FCA also published its final guidance on the rule in April 2024. The guidance outlines the FCA's expectations for sustainability references.

The "E" in ESG: Nature/Biodiversity and Taskforce on Nature-related Financial Disclosures (TNFD) – Nature is beginning to gain traction and is becoming a priority area for financial institutions, with a broad range of organisations considering nature-related risks to support robust decision-making. The financial sector plays a key role in reversing nature loss by financing nature-friendly sectors and enabling those with high land-intensive activities to transition to more sustainable practices.

The "E" in ESG: Climate risk reporting – Firms regulated by the FCA and PRA are increasingly mandated to integrate climate risk management and reporting into their operations.

Firms need to establish robust data capture systems to collect accurate and comprehensive climate-related data, and additionally, they are required to enhance their capabilities for climate risk stress testing to assess the potential impact of various climate scenarios on financial health.

The "S" in ESG: Diversity, Equity and Inclusion ('DE&I') – Pressure from customers, employees, and investors for firms to improve their DE&I was reinforced with the FCA and PRA publishing a joint consultation paper ('CP') in September 2023 setting out that firms to develop robust and evidence based DE&I strategies, set targets, and comply with annual monitoring, regulatory reporting and public disclosure requirements.

The "G" in ESG: Sustainability reporting – In the EU, the Corporate Sustainability Reporting Directive ('CSRD') represents a significant step change in how firms, at a corporate level, need to report on sustainability-related issues that are material to their business. This builds on the existing EU Non-Financial Reporting Directive ('NFRD'), but with a much wider scope, greater expectations around assurance, and far more granular standards which need to be reported against – known as the European Sustainability Reporting Standards ('ESRS') Standards.

The “E” in ESG: Net zero

Net zero continues to be a priority area for financial institutions, with many organisations making public statements about their net zero targets. In light of these targets, transition planning will be an area attracting greater scrutiny going forward from the regulators and other stakeholders such as investors and communities. In addition, in the UK, the new Labour Government has committed to introducing mandatory transition planning disclosure requirements for all FS firms. More broadly, firms are already subject to mandatory climate-related disclosure requirements aligned with the recommendations of the Task Force on Climate-related Financial Disclosures (‘TCFD’), with specific regimes for UK listed companies, UK registered companies, and regulated asset managers/asset owners.

The financial sector plays a key role in the net zero transition through financing low-carbon sectors and enabling high emitting sectors to transition to a low-carbon economy. In 2021, the previous UK Government published Greening Finance: a Roadmap to Sustainable Investing, setting out its green finance agenda. This includes plans to make transition plan disclosure the norm across the UK economy, and the UK Transition Plan Taskforce (TPT) was subsequently established to help organisations develop ‘gold standard’ climate transition plans.

The UK’s continued commitment to this was reiterated in the UK Government published Sustainability Disclosure Requirements: Implementation Update 2024. The FCA intends to consult on strengthening its expectations on transition plan disclosure with reference to the UK TPT Disclosure Framework as part of its 2025 consultation on implementing the UK-adopted ISSB standards (referred to as the UK sustainability reporting standards) for UK-listed companies.

The new labour government has also signalled its intention to continue delivering on this agenda, introducing mandatory transition plan disclosure requirements across the economy, including for all FS firms.

The TPT published its final sector-neutral Disclosure Framework on 9 October 2023, providing recommendations on developing and disclosing transition plans. In April 2024, it then published its final set of resources for businesses, which included sector specific guidance for banks, asset managers and asset owners. For the banking sector, the guidance focuses on financed and facilitated emissions associated with on and off balance sheet activities across the full range of operations and activities (e.g. lending, sales and trading, capital markets and advisory activities). For asset managers and owners, the guidance covers financed emissions, investment activities and stewardship across investment and non-investment activities. A further key development in this area, is that the ISSB has taken ownership of the body of work produced by the TPT, signalling the significance of this work.

In addition, transition plan requirements are being introduced at an EU level, notably through the EU Corporate Sustainability Due Diligence Directive (‘CSDDD’) which requires alignment with the goal of limiting global warming to 1.5 degrees Celsius above pre-industrial levels, as outlined in the paris agreement.

These requirements will apply in addition to other existing regulations and provide crucial information for clients with operations in Europe. This underscores the increasing regulatory focus on sustainability and the need for firms to integrate these requirements into their broader ESG strategies.

The “E” in ESG: Net zero (continued)

Key considerations for firms

- The firm should ensure that ensure that public statements describing how the it will achieve net zero commitments are backed by credible plans and avoid activities that could adversely affect reaching net zero, to prevent significant reputational issues.
- Firms should ensure they have adequate governance and oversight over their plans and activities for achieving net zero, which enhances accountability and increases the likelihood of successful implementation.
- The Board and senior management should ensure they have the appropriate level of knowledge to implement and monitor plans to achieve net zero, leading to better strategic decisions and increased stakeholder confidence.
- Firms should consider linking executive remuneration to sustainability goals if they have not already done so, which can drive performance and commitment at the highest levels of the organisation.
- Firms should ensure compliance with any applicable incoming transition plan requirements (e.g., under CSDDD and mandatory requirements in the UK), avoiding legal penalties and enhancing the firm's reputation as a responsible entity.
- Firms should conduct thorough and diligent financial planning and analysis with regards to their net zero planning, testing the assumptions and dependencies to assess the impact on key financial statements, ensuring financial sustainability and demonstrating a balanced approach to stakeholders.

Internal audit focus areas

- Assess whether the firm's public statements on achieving net zero commitments are backed by credible plans. Review the alignment of these plans with the firm's activities to ensure they do not adversely affect reaching net zero.
- Review the adequacy of governance and oversight over the firm's plans and activities for achieving net zero. Assess the structures in place to enhance accountability and increase the likelihood of successful implementation.
- Assess whether the Board and senior management possess the appropriate level of knowledge to implement and monitor plans to achieve net zero. Further assess whether there are training and education programs in place on Net Zero.
- Review the extent to which executive remuneration is linked to sustainability goals. Assess the mechanisms in place to drive performance and commitment at the highest levels of the organisation.
- Assess processes in place to facilitate regulatory compliance for incoming transition plans and enhancing the firm's reputation as a responsible entity.
- Assess processes in place that ensure thoroughness and diligence of financial planning and analysis related to the firm's net zero planning. Assess the testing of assumptions and dependencies to gauge the impact on key financial statements.

The “E” in ESG: Greenwashing and labels

As demand for ESG-related products and services grows, so does the risk of financial services firms potentially overstating their sustainability credentials to attract and retain customers and investors, whether done inadvertently or deliberately – referred to as ‘Greenwashing’. Regulators are already looking at greenwashing from a supervisory perspective and are also introducing explicit new rules to combat this.

Greenwashing risk can arise from statements made in a range of communications, and relate to a range of sustainability topics. Regulators across different jurisdictions are taking different approaches to defining and supervising greenwashing risks.

In November 2023, the FCA introduced PS23/16, which includes an Anti-Greenwashing rule for all FCA-authorised firms, intended to ensure all sustainability-related claims in relation to products and services are ‘fair, clear, and not misleading’. This took effect from 31 May 2024, and applies to any communication with clients in the UK in relation to a product or service.

The FCA published FG24/3, its Finalised non-handbook guidance on the Anti-Greenwashing Rule, in April 2024. The guidance outlines the FCA's expectations for sustainability references, including that:

- They are **correct** and capable of being substantiated.
- They are **clear** and presented in a way that can be understood.
- They are **complete**, i.e. do not omit or hide important information, and consider the full product/service life cycle.
- **Comparisons** to other products/services are **fair** and **meaningful**.

As part of its new UK Sustainability Disclosure Requirements (SDR) regime, the FCA has introduced a new sustainable investment product labelling framework for asset managers (See PwC's joint report with UK SIF on SDR implementation for asset managers here). This contains four distinct, voluntary sustainable investment labels intended to set minimum requirements for labelled funds to comply with (see PwC’s summary here).
The intention is to provide investors with greater understanding of, and confidence in, the sustainability credentials of the funds they invest in. The earliest point that firms could apply a label to their funds was 31 July 2024. For any unlabeled products, the FCA introduced 'naming and marketing' rules for funds, which intended to enhance the accuracy of sustainability references and claims, these rules take effect from December 2024.

This follows an active EU agenda in this area. The Sustainable Finance Disclosure Regulation (SFDR) has introduced disclosure requirements in relation to so-called Article 6, 8 and 9 products. While not a formal labelling framework, in practice this regulation has in recent years shaped how asset managers have been making decisions around their sustainability-related product offerings. Alongside SFDR, in 2024 the European Supervisory Authorities (ESAs) finalised fund naming guidelines for asset managers, which are intended to establish more consistency in the way that products are marketed from a sustainability perspective to help protect against greenwashing risk.

The “E” in ESG: Greenwashing and labels (continued)

Key considerations for firms

- AWM firms should ensure they have an internally-agreed-upon definition of greenwashing and adopt a consistent approach across the organisation to identify and mitigate greenwashing risks. This will ensure products are appropriately classified under relevant regulations (e.g., Sustainable Disclosure Regulation (‘SDR’), Sustainable Finance Disclosure Regulation (‘SFDR’), and European Securities and Markets Authority (‘ESMA’) fund naming guidelines), thereby mitigating the risk of greenwashing accusations.
- There should be clear roles and responsibilities within the firm in relation to greenwashing risks, including accountability for greenwashing risk. This reflects that the firm understands greenwashing as a risk to the business.
- There should be appropriate governance and oversight over sustainability-related claims made externally and the voluntary commitments, frameworks, and industry groups the organisation signs up to. This ensures that the organisation’s public statements and affiliations genuinely reflect its practices and values.
- ESG-related policies, procedures, and risk and control frameworks should adequately consider greenwashing risk. This ensures that products and services are managed in a way that aligns with their sustainability profile, preventing misalignment and reinforcing the firm’s commitment to genuine and transparent sustainability practices.
- Sales and marketing staff should be adequately upskilled on the permitted terms they can use in relation to sustainability when communicating with clients. This training helps prevent the inadvertent use of misleading or exaggerated claims that could be construed as greenwashing.
- Firms should ensure that products qualify for labels under different regimes to avoid challenges in external communications regarding the firm’s (global) approach to ESG. For example, firms need to be able to explain why a product is considered sustainable under one regime but not under another. This helps maintain consistency and transparency in the firm's sustainability communications and practices.

Internal audit focus areas

- Assess whether greenwashing risk is incorporated into the firm’s controls and risk management frameworks, as well as the framework for classifying products under key regulations.
- Assess whether appropriate roles and responsibilities for greenwashing risk are clearly defined and implemented, and assess whether there is appropriate senior management oversight.
- Review the controls for ensuring that disclosures and reporting are appropriate based on the given label/classification of a product..
- Review ESG-related policies and procedures and assess whether they adequately consider greenwashing risks.
- Review training plans for marketing staff and assess whether they adequately cover permitted terms to use regarding sustainability, and assess whether training is provided.
- Assess ESG-related external commitments made by the firm and whether there is a credible plan in place to meet these commitments, and further assess that sustainability-related claims are in line with FCA anti-greenwashing rules and guidelines.
- Review processes for ongoing monitoring of investments/product features to ensure alignment with classifications/labels.

The "E" in ESG: Nature/Biodiversity and TNFD

Nature is becoming a priority area for financial institutions, with a broad range of organisations considering nature-related risks to support robust decision-making. In addition to climate targets such as net zero, organisations are now assessing risks and setting targets in other domains such as biodiversity, oceans, land, and freshwater in an effort to mitigate business risk and help reverse nature loss. Organisations with land-intensive activities in their value chains will be expected to set a Forest, Land, and Agriculture ('FLAG') target, which includes committing to zero deforestation. The financial sector plays a key role in reversing nature loss by financing nature-friendly sectors and enabling those with land-intensive activities to transition to more sustainable practices. Through strategic investments and lending policies, financial institutions can support the development of industries that prioritise environmental sustainability and encourage companies to adopt practices that protect and restore natural ecosystems.

The Taskforce on Nature-related Financial Disclosures (TNFD) builds on the Task Force on Climate-related Financial Disclosures ('TCFD') framework and aligns with emerging standards from organisations like the ISSB and SBTN (more below). In September 2023, the TNFD published its recommendations and while TNFD requirements are currently voluntary, there is increasing momentum to make them mandatory, similar to TCFD. The TNFD introduced the LEAP (Locate, Evaluate, Assess, Prepare) nature-risk management process and includes fourteen recommended disclosures, closely aligned with TCFD but with adjustments to account for the spatial dimensions of nature.The fourteen disclosures are grouped under four pillars.

- **Governance:** Describe the Board's oversight and management's role in assessing and managing nature-related risks and opportunities.
- **Strategy:** Outline nature-related risks and opportunities over the short, medium, and longer term, their impact on business and financial planning, and the resilience of the organisation's strategy considering different scenarios.
- **Risk management:** Detail the processes for identifying, assessing, and managing nature-related risks, and how these processes are integrated into overall risk management.
- **Metrics and targets:** Disclose the metrics and targets set to manage nature-related risks and opportunities, and report performance against these targets.

The language in Global Biodiversity Framework (GBF) Target 15 – mirrors the TNFD and requires national governments to make it mandatory for large and transnational companies to regularly monitor, assess, and disclose their nature-related risks, dependencies, and impacts.

The CSRD includes four nature-related standards, namely: Pollution, Water, Biodiversity and Ecosystems, and Circular economy.

The International Sustainability Standards Board (ISSB) – Has announced its plan to develop new standards focused on biodiversity. Key aspects of the ISSB's biodiversity standards are expected to include: assessment of biodiversity impacts, Biodiversity management practices, Dependency on biodiversity, reporting and transparency and alignment with global initiatives. It is highly likely that the ISSB will build on the work of the TNFD.

The Science Based Targets Network (SBTN) – Among its various focus areas, has developed specific targets for land and water to help organisations contribute to the sustainable management of these vital resources. These targets are grounded in the latest scientific research and are designed to align with global sustainability goals.

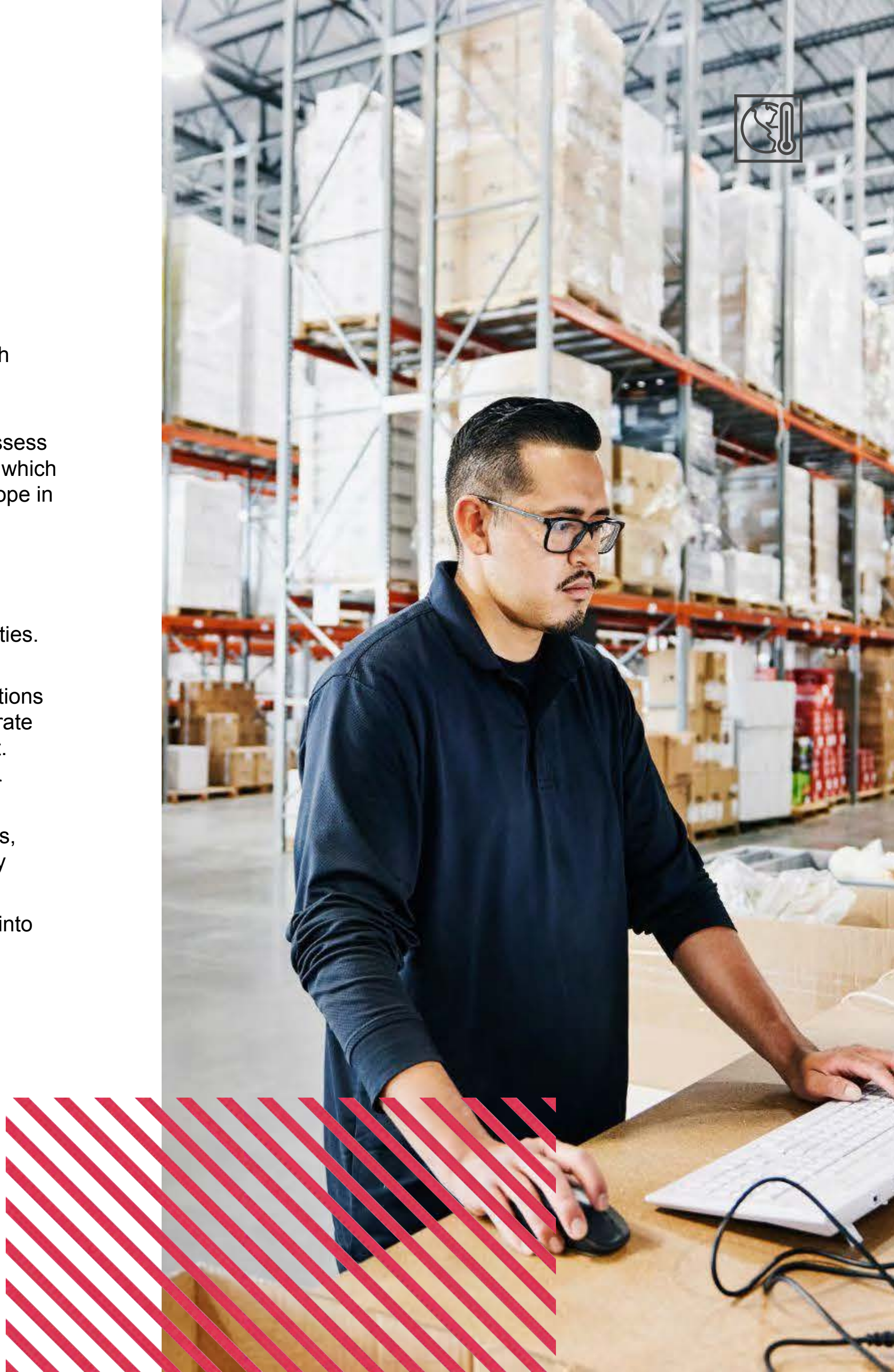
The "E" in ESG: Nature/Biodiversity and TNFD (continued)

Key considerations for firms

- Firms should set out their approach to materiality, ensuring alignment with external standards or regulatory requirements where appropriate, which enhances credibility and ensures regulatory compliance.
- Firms should provide a description of the scope for the disclosures, ensuring coverage of both the business and the value chain. If disclosing against the TNFD framework, firms should identify which disclosures have been addressed and outline plans to extend this scope in the future, thereby demonstrating transparency and forward-thinking to stakeholders.
- Firms should identify nature-related risks and opportunities based on an assessment of dependencies and impacts on nature, which enables proactive risk management and the identification of potential opportunities, strengthening the firm's strategic positioning.
- Firms should ensure that the specific locations of their interface with nature are integral to the assessment process, which provides a more accurate and relevant understanding of their environmental impact, aiding in more targeted and effective sustainability strategies.
- Firms should ensure that nature-related disclosures are integrated with other sustainability-related disclosures, including climate-related disclosures, with any alignment, contributions, and possible trade-offs clearly identified, which fosters a holistic view of sustainability efforts and enhances stakeholder trust.
- Firms should ensure that stakeholder engagement is taken into account across all disclosures, which improves the relevance and acceptance of the disclosures, and enhances the firm's reputation and relationships with its stakeholders.

Internal audit focus areas

- Assess the firm's approach to materiality and how it aligns with external standards or regulatory requirements.
- Review the firm's description of the scope for its disclosures, and how they cover both the business and the value chain. Assess the firm's compliance with the TNFD framework by identifying which disclosures have been addressed and plans to extend this scope in the future.
- Assess the processes for identifying nature-related risks and opportunities based on an assessment of dependencies and impacts on nature. Assess their effectiveness in enabling proactive risk management and identifying potential opportunities.
- Review the firm's assessment of specific locations where it interfaces with nature. Further assess how integral these locations are to the overall assessment process to ensure a more accurate and relevant understanding of the firm's environmental impact.
- Assess the integration of nature-related disclosures with other sustainability-related disclosures, including climate-related disclosures. Review the clarity of any alignments, contributions, and possible trade-offs to foster a holistic view of sustainability efforts and enhance stakeholder trust.
- Review the extent to which stakeholder engagement is taken into account across all disclosures and assess the processes for engaging stakeholders.



The “E” in ESG: Climate risk reporting, including capture of climate data in control environments and climate risk stress testing

Firms regulated by the FCA and the PRA are increasingly required to integrate climate risk management and reporting into their operational frameworks. Key aspects of compliance include the identification and assessment of climate risks, which encompass both physical risks (e.g., extreme weather events) and transition risks (e.g., shifts towards a low-carbon economy). These risks must be incorporated into existing risk management practices and considered alongside traditional financial risks.

To manage climate risks effectively, institutions must establish robust data capture mechanisms within their control environments:

- Collecting and analysing relevant data on climate-related exposures, such as emissions data, energy consumption, and the geographical locations of assets.
- Ensuring that this data is accurate, comprehensive, and integrated into risk management systems is crucial.
- Additionally, firms are required to enhance their capabilities for climate risk stress testing, which involves simulating various climate scenarios to assess their potential impact on financial health. These stress tests help understand the resilience of portfolios under different climate conditions and inform strategic decision-making.

The PRA supervisory statement 3/19 (SS3/19), launched in 2019 with a compliance deadline in 2021, has been supplemented by subsequent Dear CFO (‘Chief Financial Officer’) letters in 2022 and 2023, as well as Written Auditor Report summary findings. These reports further clarify the PRA's expectations regarding the management of financial risks arising from climate change.

They include examples of effective and less effective practices and provide recommendations for the short and medium term, such as:

- Incorporating climate considerations into performance reporting processes.
- Incorporating climate considerations into balance sheet valuations.
- Enhancing risk management capabilities.
- Enhancing data governance.

The “E” in ESG: Climate risk reporting, including capture of climate data in control environments and climate risk stress testing (continued)

Key considerations for firms

- Firms should ensure that they enhance analytical capabilities and dynamic balance-sheet modeling abilities for measuring financial impacts arising from climate change to meet increasing expectations from regulators. This enhances the firm's ability to assess and report on climate-related financial risks accurately.
- Firms should ensure there is management ownership and adequate oversight over methodologies, assumptions, and limitations of vendor models and in-house solutions. This ensures that the firm’s modeling practices are transparent, credible, and robust.
- Firms should consider the incorporation of climate risk in ICAAP, IFRS 9 and IRB models, financial planning solutions, and risk appetite frameworks. This ensures that climate risk is integrated into the firm’s overall risk management and financial planning processes.
- Firms should ensure that they have key processes in place to monitor and keep up to date with the regulatory agenda and expectations that are constantly evolving, to be aligned with the PRA’s expectations of high-quality practices. This ensures that the firm remains compliant and aligned with the latest regulatory requirements and best practices.
- Firms should ensure that they have capabilities for measuring carbon footprint (Scope 1, 2, 3) including baselining and forecasting, underpinning assumptions, data quality, alignment with market practice, and relevant standards (e.g., PCAF). This ensures the firm’s carbon footprint measurements are accurate, comprehensive, and in line with industry standards and expectations.

Internal audit focus areas

- Assess the firm’s enhancement of analytical capabilities and dynamic balance-sheet modeling abilities for measuring financial impacts arising from climate change and their adequacy to meet increasing regulatory expectations.
- Review the management ownership and oversight over methodologies, assumptions, and limitations of vendor models and in-house solutions. Assess the transparency, credibility, and robustness of the firm’s modeling practices.
- Assess the incorporation of climate risk into ICAAP, IFRS 9, and IRB models, financial planning solutions, and risk appetite frameworks. In addition assess processes in place to ensure climate risk is effectively embedded into the firm’s overall risk management and financial planning.
- Review the firm’s processes for monitoring and keeping up to date with the evolving regulatory agenda and expectations. Assess the alignment with the PRA’s expectations of high-quality practices to ensure the firm remains compliant and aligned with the latest regulatory requirements and best practices.
- Assess the firm’s capabilities for measuring carbon footprint (Scope 1, 2, 3), including baselining and forecasting. Assess the underpinning assumptions, data quality, alignment with market practice, and adherence to relevant standards (e.g., PCAF) to ensure the firm’s carbon footprint measurements are accurate, comprehensive, and in line with industry standards and expectations.

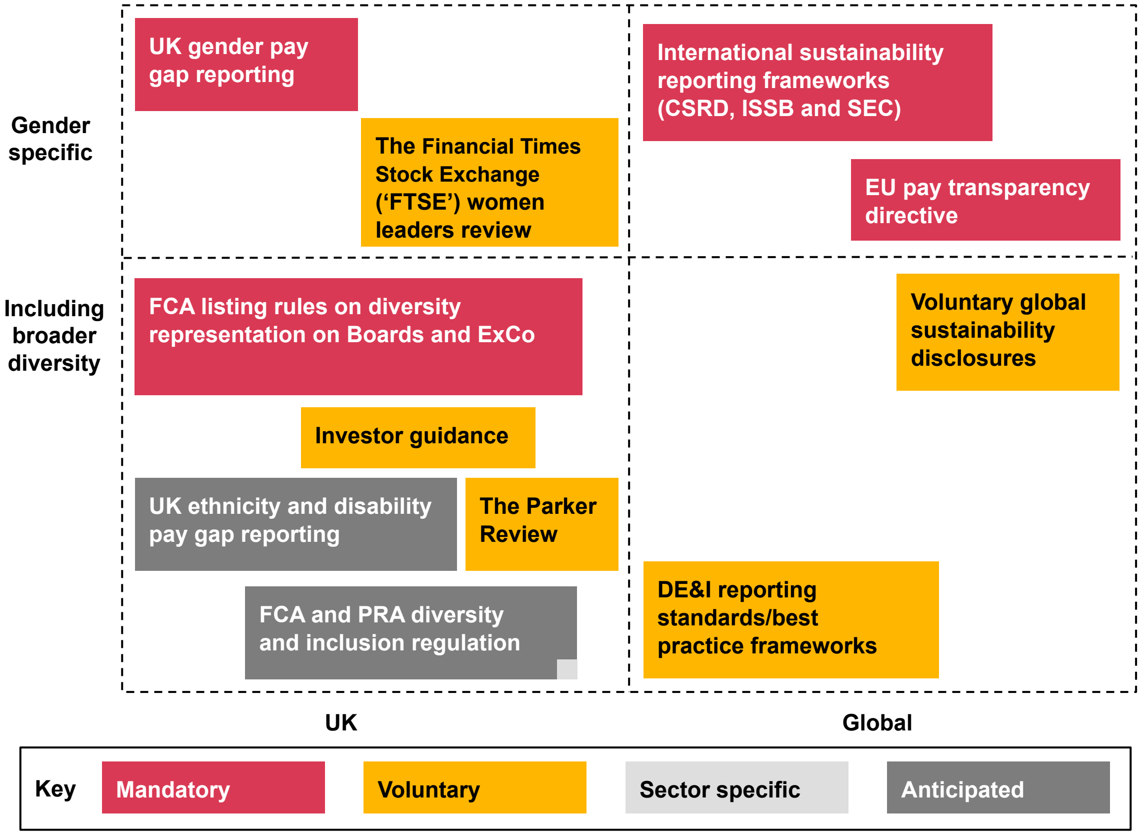
The “S” in ESG: Diversity, Equity and Inclusion (‘DE&I’)

In recent years, DE&I has catapulted up the business priority list due to shifting societal norms, an increasing legislative and regulatory focus in the UK and Europe and a growing body of research outlining its benefits to productivity, profitability and innovation. However, firms can easily miss the mark with ‘off the shelf’ initiatives and training programmes, even with considerable investment. DE&I ambitions should be pursued in a strategic, data-driven manner – same as any other business goal.

Pressure from customers, employees, and investors for FS firms to improve their DE&I programs has been building in recent years.

This was reinforced in September 2023* with the publication of the FCA and PRA joint CP. The CPs included proposed requirements for firms to develop robust and evidence based DE&I strategies, set targets, and comply with annual monitoring, regulatory reporting and public disclosure requirements. The CPs also reinforced that a lack of diversity may be considered a non-financial business risk for firms. The final policy statement has not yet been published, however the CPs indicate that the regulators increasingly expect to see DE&I risk to be treated within risk and governance structures with the same rigour as any other business risk, regardless of firm size.

There are also a number of new and incoming non-sector specific laws and regulations which will impact many firms (see below), e.g. the EU pay transparency directive will expand equal pay law across the EU, amongst other requirements, CSRD will require diversity data reporting and increased disclosure of misconduct, and the UK ethnicity and disability pay gap reporting requirements will mean that firms will have to broaden their DE&I efforts beyond gender.



It is important that organisations **do not let this evolving landscape become a compliance exercise**; instead, reporting and transparency should be embraced as a means to increase productivity, fairness and talent attraction, and organisations should focus on implementing actions that will drive meaningful change.

To do so, many firms will need to invest by gathering robust diversity and inclusion data, upskilling their people and ensuring they have appropriate governance frameworks in place to deliver their DE&I strategies.

*more detail can be found here: https://www.pwc.co.uk/human-resource-services/assets/pdfs/fca-and-pra-consultation-papers-diversity-inclusion.pdf

The “S” in ESG: Diversity, Equity and Inclusion (‘DE&I’) (continued)

Key considerations for firms

- Firms should gather adequate data and take suitable actions to meet DE&I regulations to avoid the risk of losing or suspending licenses and/or facing restrictions on accessing the market.
- Firms should ensure effective prevention of discrimination and/or non-financial misconduct. This helps mitigate the risk of such information becoming public, which can cause severe reputational damage, making it difficult to attract talent and clients, and damaging consumer confidence and public perception of the sector.
- Firms should address discrimination, bullying, and other non-financial misconduct as these can be indicators of low honesty and integrity in leaders and/or employees. The FCA and PRA have highlighted this as a broader conduct risk that can adversely impact confidence and trust in the industry, potentially leading to market instability.
- Firms should ensure compliance with legislation such as equal pay law and the Equality Act 2010 to avoid the risk of significant fines and/or legal costs.
- Firms should promote diversity in decision-making roles to avoid 'groupthink,' which can result from a lack of cognitive diversity and differing viewpoints. This is essential to ensure effective decision-making, optimise business performance, and increase profits.
- Firms should implement equitable processes to ensure high-performing employees are appropriately recognised, promoted, and retained. Failure to do so can hinder overall business performance and lead to a culture lacking in inclusivity, increased employee turnover, impacting business continuity, staff morale, and operating costs.

Internal audit focus areas

- Conduct a regulatory gap assessment to identify gaps in compliance against developing legal and regulatory requirements (e.g. FCA/PRA D&I requirements, CSRD, etc.).
- Conduct a maturity assessment of the firm’s existing DE&I strategy and associated processes (to be scoped in as required/relevant) using PwC DE&I maturity model to identify key areas for improvement.
- Assess the effectiveness of firm’s processes in place to deliver on their DE&I commitments, including the delivery/action plans in place, processes to track, monitor and evaluate progress and governance framework.
- Assess the suitability and appropriateness of firm’s DE&I strategy, including identifying whether it is appropriate given relevant regulatory requirements, and whether appropriate inputs were considered when developing the strategy.
- Assess organisational processes, e.g. recruitment and selection, promotions, employee conduct, etc, to determine whether they are adequately inclusive and whether there are appropriate controls in place to mitigate biases.
- Conduct an assessment of the firm’s culture through senior leadership interviews and employee listening to deep-dive on known challenges, e.g. leadership behaviors, employee conduct, etc, to identify root causes and develop targeted actions to address them.

The “G” in ESG: Sustainability reporting

Sustainability reporting is still a key area of focus, driven by new regulations, investor pressure, and strategic priorities. FS firms face a wave of sustainability reporting regulations beyond climate, notably the EU’s CSRD and the UK's evolving framework.

FS firms are facing a flurry of new sustainability reporting regulations and standards, spanning the full spectrum of sustainability factors – beyond just climate.

In the EU, the CSRD represents a significant step change in how firms, at a corporate level, need to be reporting on sustainability-related issues that are material to their business. This builds on the existing EU Non-Financial Reporting Directive (NFRD), but with a much wider scope, greater expectations around assurance, and far more granular standards which need to be reported against – known as the ESRS Standards. Given the expanded new scope of CSRD compared to NFRD, many UK-based entities of FS groups will be impacted by this significant regulation.

On 16 May 2024, the previous UK Government published an Implementation Update on its Sustainability Disclosure Requirements (‘SDR’) regime, outlining expected timings for taking forward the economy-wide sustainability reporting framework originally launched in Greening Finance: a Roadmap to Sustainable Investing. This SDR regime is intended to build on mandatory task force on climate-related Financial Disclosures (‘TCFD’) reporting in the UK, and would apply to UK listed companies, UK registered companies, and FCA regulated asset managers.

The ambition of the regime is to introduce decision-useful sustainability disclosures through the investment chain. The implementation update noted that new entity and product level disclosure requirements for asset managers have already been finalised by the FCA.

At a corporate level, the previous Government introduced a framework for developing UK-adopted versions of the International Sustainability Standards Board (‘ISSB’) Standards, termed the UK Sustainability Reporting Standards (‘SRS’). A technical advisory committee has been established to assess the ISSB Standards in Q2 2024, with recommendations due by Q4 2024, followed by a UK Government consultation on draft UK SRS in Q1 2025. Once finalised, the FCA will consult on disclosure requirements for UK-listed companies and the Government will determine requirements for other companies (including any listed or unlisted FS firms).

Additionally, the Implementation Update confirmed there will be a consultation on the UK green taxonomy's overarching framework, use cases, and activity-level criteria, with voluntary disclosure for at least two years before considering mandatory disclosures.

In advance of the 2024 general election, Labour signaled that it remains committed to delivering the UK Sustainability Disclosure Requirements (‘SDR’) framework and the UK green taxonomy, indicating this will be a continued focus for the new Government.

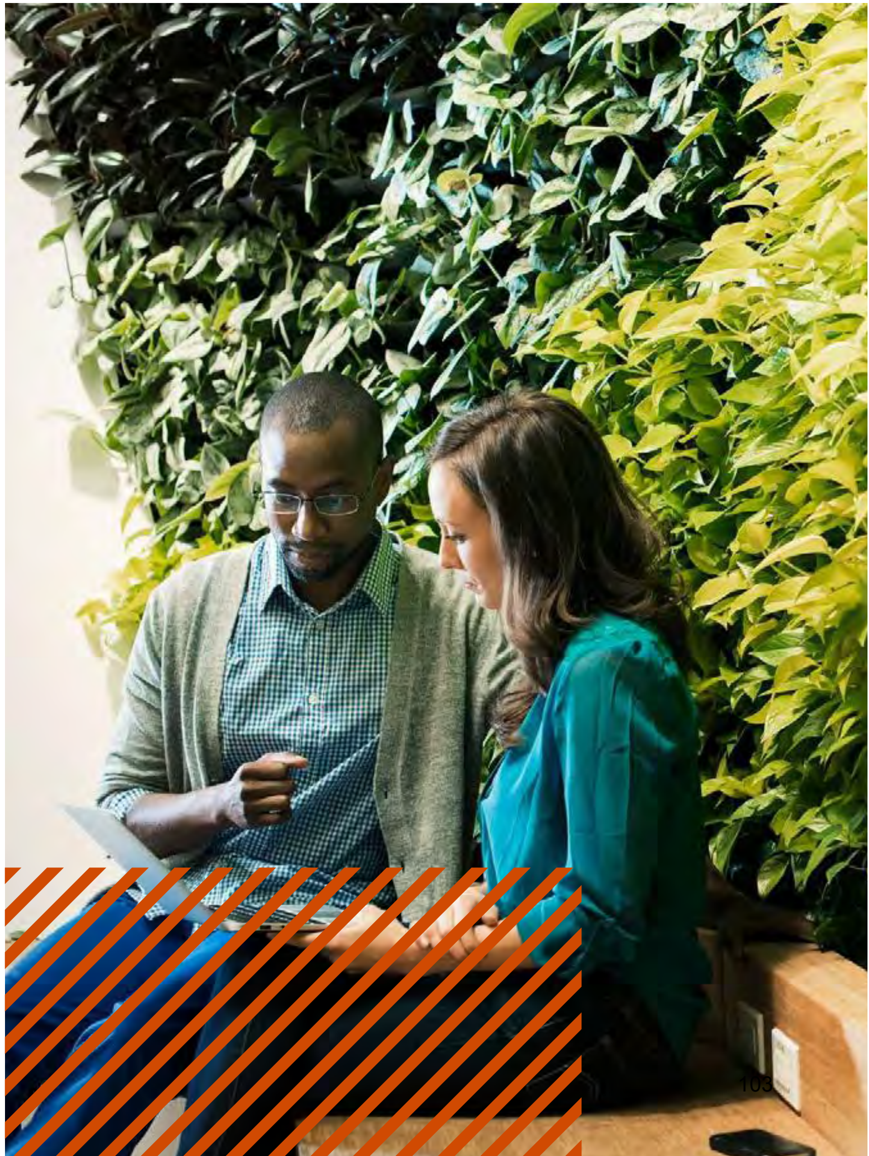
The “G” in ESG: Sustainability reporting (continued)

Key considerations for firms

- Firms should ensure there is robust governance and structure around understanding and implementing sustainability initiatives across the organisation.
- The firm should have a clear strategy and timeline to meet regulatory requirements, understanding what to do and when, to avoid missing deadlines.
- Strategies should be developed to meet investor expectations and address activist pressures, thereby preventing potential reputational and financial losses.
- Reporting should be underpinned by a robust materiality assessment framework to provide decision-useful disclosures for investors and other stakeholders.
- Firms should have a materiality assessment methodology that incorporates both financial materiality (how sustainability issues affect its financial performance) and environmental and social materiality (how its operations impact the environment and society). This methodology should consider industry standards, regulatory requirements, and emerging trends, using a combination of qualitative and quantitative data sources to identify and prioritise material issues.
- Entities in scope of the CSRD should have robust and documented processes for assessing materiality, gathering data, and generating reports that can withstand assurance scrutiny.

Internal audit focus areas

- Assess the robustness of the governance and structure around understanding and implementing sustainability initiatives across the organisation. This includes evaluating the clarity of roles and responsibilities, the effectiveness of sustainability committees, and the integration of sustainability into the overall corporate governance framework.
- Review the firm’s strategy and timeline for meeting regulatory requirements, ensuring there is a clear understanding of what needs to be done and when, to avoid missing deadlines. This includes assessing the processes for tracking regulatory changes and implementing necessary actions in a timely manner.
- Assess the strategies developed to meet investor expectations and address activist pressures, thereby preventing potential reputational and financial losses. This includes evaluating the effectiveness of stakeholder engagement processes and the responsiveness of the firm to investor and activist concerns.
- Review the robustness of the materiality assessment framework underpinning the firm’s reporting to provide decision-useful disclosures for investors and other stakeholders. This includes assessing the processes for identifying, prioritising, and validating material sustainability issues.
- Assess the firm’s materiality assessment methodology including how it incorporates both financial materiality and environmental and social materiality. Assess alignment with industry standards, regulatory requirements, and emerging trends, as well as the use of qualitative and quantitative data sources.
- Review the robustness and documentation of processes for assessing materiality, gathering data, and generating reports for entities in scope of the CSRD.



Professional practices update

The IIA's Global Internal Audit Standards™

The new Global Internal Audit Standards were released by the Institute of Internal Auditors ('IIA') in January 2024 and are expected to be implemented by all firms by 9 January 2025. They replace the existing international professional practice framework, including the standards, last revised in 2017. There is a very different structure to the new Standards, which are centred around five domains, with each one designed for a different group of users. For example, Domain V is more likely to be used by the audit delivery teams in your function. More information on the domains can be seen in the following pages. Within the new domains and their 15 principles and 52 standards, there is a large degree of consistency with the previous International Professional Practices Framework ('IPPF') and some requirements where the expectations are more defined.

Some of the key areas of change for financial services ('FS')

The new Standards will present different challenges for each organisation as it compares its current practices to the new requirements. We have highlighted just three of the areas below where, in our experience, many firms are seeing the biggest changes in practice.

Board and senior management responsibilities

The UK's FS Code has always set a high expectation for the involvement of the Board/Audit Committee in the governance of the internal audit function and the management of the chief audit executive. However, the requirements have been less precise for other organisations. Domain III focuses on these in areas and sets clear expectations for the involvement of Senior Management in IA strategy, the resourcing of internal audit, the objectives and assessment of the chief audit executive, and in the scoping and outcome of the external quality assessment.

These stakeholders should be brought up to speed and involved by internal audit functions as early as possible, to collectively respond to the requirements of the Standards, and to gain value from this more joined up approach.

Internal audit strategy

In order to conform with the new Standards, internal audit must develop and implement a strategy for the function that is aligned to the overall strategy of the organisation, and to discuss this with the Board and Senior Management at least annually. For many functions, especially larger functions and/or those with a continuous improvement focus, a strategy will already be in place. However, it has never been a requirement of the IPPF or the FS Code and, in our experience there are a number of functions - large and small - without an internal audit strategy. The requirement to present on the strategy to the Board and Senior management at least annually should encourage the use of the strategy as a living document that helps drive growth and continuous improvement.

Internal audit expected behaviours

For the first time, the Standards refer to the need for professional scepticism. Additionally, Domain II places an emphasis on 'professional courage', 'communicating truthfully' and 'taking appropriate action' for expected behaviours of auditors, and for the chief audit executive to maintain a work environment where internal auditors feel supported when expressing legitimate, evidence-based engagement results, whether favourable or unfavourable.

These standards reflect good practice and we recommend that teams actively reinforce these core messages through training and communications. Most importantly, teams should ensure that they have mechanisms in place to monitor and measure whether the training, communication, etc. are having the desired outcomes. Teams may be able to leverage their existing quality assurance processes to do so, including regular reporting of the results.

The IIA's Global Internal Audit Standards™ (continued)

The implications for financial services ('FS') internal audit

- For those in FS, in particular those subject to sector-specific requirements, such as the UK FS Code, some of the new requirements will not be new at all. Many of them are already commonly adopted practice, such as Standard 14.5, which requires for internal audit reports to have an overall rating.
- We believe that the new Standards will not require much change in day-to-day practice for many mature internal audit functions, but even where change in practice may not be required, work is needed to demonstrate conformance. For example, with the ethics and professionalism requirements of Domain II and the requirements of parties outside of internal audit – namely the Board and Senior Management – in Domain III (see overleaf).
- Internal audit functions will need to decide on and document their interpretation of and response to some of the requirements that may be subjective or not currently followed 'to the letter' – for example, those in Domain V regarding the review of 'engagement documentation' by the chief audit executive.
- However, there are some new or evolved areas not just for internal auditors, but also quite specifically for the Board and Senior Management, as set out in Domain III – **Governing the internal audit function**. This domain sets out requirements for the Board and Senior Management for their involvement in the strategy, mandate, resources, quality and independence (amongst others) of internal audit in a way that is completely new from the IPPF, is more formalised and explicit than many organisations have in practice, and that in many areas, such as strategy, goes beyond the requirements of the Board made by the FS Code.
- It is these requirements under the Governance domain in particular that provide the greatest opportunities for internal audit functions and their stakeholders to elevate the value that internal audit provides and to better align internal audit's mandate and delivery with stakeholder needs. For some examples of this, refer to the following pages.

The IIA's Global Internal Audit Standards™ (continued)

Below are our perspectives on the requirements of the five domains and their 15 principles and 52 standards.

Domain I
Purpose of internal auditing

This replaces the Mission and Definition within the IPPF. There are notable changes in the wording, however, in essence the purpose of internal audit remains largely the same, with more focus on 'create, protect and sustain values', and bringing 'foresight' to stakeholders.

A key change is the introduction of the need for internal audit to provide 'foresight'. This is also reflected in the CIIA's revised internal audit code of practice published in September 2024.

It is a very short domain, with no principles or standards.

Domain II
Ethics and professionalism

This replaces the Code of Ethics within the IPPF, but goes much further, setting out the expected behaviours of all individuals responsible for the delivery or governance of internal audit activities. This domain will require attention from functions, largely in order to formalise the policies, procedures and controls that are likely already in place, but also to consider how it will demonstrate conformance with the five principles and 13 standards in this domain.

We recommend that functions consider the desired outcomes of this domain and not just the processes, including how they will assess and measure the extent to which these outcomes are being achieved over time, and take corrective action as needed. For example, functions may with to use the quality assurance process to assess whether the intentions of the ethics and professionalism standards are being met and routinely demonstrated on individual audit engagements and wider.

Domain III
Governing the internal audit function

This domain will likely necessitate the most change. The three principles and nine standards in Domain III are for the Board and Senior Management, and not for internal audit. Many of the expectations are already a requirement of the FS Code and others are common practice, but some, including the requirement for Senior Management to discuss with and provide input to the the Board and chief audit executive regarding the expectations for the internal audit function when setting its mandate is not consistently seen across all functions.

Internal audit teams will need to work with the Board and Senior Management to determine how these standards should be interpreted, enacted and demonstrated. We recommend that Chief Internal Auditors should start talking to their Audit Committee Chairs and CEOs ('Chief Executive Officer') now, if they haven't already done so, about the new Standards and their responsibilities, before taking them to the wider AC/Board and Senior Management. In some organisations, it may take time to get all senior stakeholders comfortable with where internal audit is positioned today and its plans for the future, especially if there is work to do.

Despite the challenges, this domain has the potential to yield the biggest benefits for some organisations. By clarifying and formally agreeing the mission and mandate of internal audit and the support and engagement needed from the Board and Senior Management, there is potential for greater alignment. This in turn should foster confidence, allowing teams to deliver their work with purpose and conviction.

The IIA's Global Internal Audit Standards™ (continued)

Domain IV
Managing the internal audit function

This domain includes four principles and 16 standards focussed on the strategy, operations, communication and quality arrangements of the internal audit function.

A key change is the requirement to develop and implement an internal audit strategy that supports the organisation's strategy, objectives and success, and that aligns with the expectations of the key stakeholders. Many internal audit functions do not have a strategy. The requirement is intended to encourage continuous improvement and innovation.

It also includes more emphasis on building trust and relationships with stakeholders in the business, rather than a focus on pure independence, which we see as a positive step.

It includes the development of a risk-based internal audit plan, where little has changed except for the need to include considerations of certain risks, such as governance and IT. No changes are seen in the areas of working with/reliance upon other assurance providers.

Domain V
Performing internal audit services

This domain contains three principles and 1 standard, and focuses on the delivery of individual engagements (audits / reviews / assessments / etc.). The requirements are largely in line with common practice. For example, Standard 14.3 Evaluation of Findings requires internal audit to consider the risk associated with the finding and to prioritise (i.e. rate) each finding. The difference in this standard and common practice may be the requirement to "collaborate with management to identify the root causes". Root cause is done well by some, but could be improved by most, and many functions don't necessarily work collaboratively with the business to identify true root cause. Internal audit should consider how this is interpreted, particularly where root causes might be complex and there is disagreement. Some functions might wish to undertake additional training, update their methodology, and / or allocate additional time to deliver audits and communicate with the business in relation to these subtle but important changes.

Another feature of this domain is that teams will need to make clear decisions on how exactly to interpret and implement requirements. For example, Standard 14.6 Engagement Documentation requires that the chief audit executive reviews and approves engagement documentation. Outside of very small functions, this is often a role that is delegated to audit leaders or managers, and to change this approach may not be seen as practical/the optimal use of team resources. In this and some other areas, we advise that teams should document their approach and how it complies with the principle of the standards, if not the exact wording.

The IIA's Global Internal Audit Standards™ (continued)

Key actions for internal audit teams to consider now

01 **Plan and assess**

Perform a readiness assessment and decide on your desired response. Expect that some areas will be easily addressed, but others will take time and require stakeholder engagement, decisions on approach, methodology changes and training.

02 **Engage key stakeholders early**

Speak to your Audit Committee Chair and Chief Executive as soon as possible. Brief them on the new Standards and their responsibilities under Domain III. Agree on a plan to involve the wider Board and Senior Management. You will need their buy-in to changes and support if you need additional resources to deliver those changes.

03 **Look at the wider 3LOD and mandate**

Use this as an opportunity to consider your mandate within the organisation as a whole, collectively working with the other lines of defence to shape the future model and assurance framework.

04 **Decide on approach to regulated local entity needs**

For those in groups with multiple regulated entities and Boards, consider how your local entity heads of internal audit will respond to the Standards, especially what you expect of smaller teams.

05 **Make the underlying changes**

Work through your methodology, systems, QA, etc. to update them for the new Standards. This will take time and may flush out areas whether more work is needed to get ready, so start early. Document your interpretation of any areas of subjectivity.

06 **Pilot and test the changes**

Select a pilot project in your 2024 Audit Plan to trial your proposed updates as a test run before going live in 2025.

07 **Assess readiness pre-go live**

Consider a pre-go live external assessment to test the robustness of your response, suggest final remediation activities and provide assurance to internal audit and its stakeholders that you are ready for day 1.

The IIA's Global Internal Audit Standards™ (continued)

What we would expect be reported to the audit committee

01 An overview of the new standards, including Board and Senior Management responsibilities – **now.**

02 Gap analysis and remediation plan – **by autumn 2024.**

03 Conformance self assessment – **by January 2025.**

Where to find more information

Read more on the PwC website.

Download the new standards on the IIA's global website.

Download the condensed standards rom the IIA's global website.

Download mapping of the 2017 IPPF to the 2024 standards.

Read PwC's Global Internal Audit Study: Seeing through walls to find new horizons

Things to look out for in the coming months

Future editions of PwC's Reframe IA series on our website, helping you to leverage the opportunities presented by the new Standards.

Future Topical Requirements from the IIA. These set out the requirements when providing assurance on a specified risk area. The first one, on the audit of Cyber, has been released.

The Quality Assessment Manual from the IIA, due later in 2024, which we understand is due to set out further expectations on the Standards and assessing conformance with them against a new rating scale.

The CIIA combined Internal Audit Code of Practice

Following an eight-week extensive consultation period, the Chartered Institute of Internal Auditors (‘CIIA’) released the new Internal Audit Code of Practice in September 2024. The Code sets out fundamental principles for running a strong and effective internal audit function.

Effective from January 2025, the Code will be applicable to all internal audit functions in the financial services, private and third sectors, in alignment with the new Global Internal Audit Standards and the revised UK Corporate Governance Code.

As our profession navigates an increasingly more uncertain, risky and rapidly changing world, the release of the new Code is particularly timely. It provides an opportunity to strengthen the role of internal audit in assisting boards and senior management with identifying, managing and mitigating risks effectively in a dynamic landscape. The CIIA believes that this Code will be instrumental in moving our profession forward and enhancing corporate governance.

The Code includes a set of 37 principles: five are new, five are unchanged, of the remaining 27, 15 have only minor wording changes whilst the other 12 have changes that are likely to have some impact on internal audit functions and their stakeholders.

Key differences

Some of the changes include:

- **Principle 3**: The chief audit executive should report annually to the Board audit committee on the application of the Code’s principles, focussing on outcomes rather than a self-assessment against the code.
- **Principle 4**: The organisation’s board audit committee report in the annual report and accounts should summarise the purpose and mandate of internal audit, the function’s main activities and conclude on internal audit’s impact and effectiveness. There may be a variety of inputs to this assessment, such as internal audit’s quality assurance programme and its self-assessments. The assessment provides an opportunity for the CAE and the board audit committee to reflect on an annual basis on the impact the function delivers.
- **Principle 6**: Risk assessments and prioritisation of internal audit work. The wording removes references to cyclical coverage of the audit universe, instead allowing for purely risk-based plans. The wording explicitly includes regulators as a stakeholder group from whom internal audit should obtain views during the risk assessment process. Additionally, **Principle 7.** Internal audit coverage and planning places a focus on dynamic audit planning.
- **Principle 8a, f, h, i, j:** Includes new required areas of scope: purpose, ESG, financial crime, economic crime and fraud, and technology, cyber, digital and data risks. In addition, key external events are now required to be considered within scope. The majority of these will already be included in the plans of many functions, but the requirement on auditing against purpose is new. This new requirement is intended to support the role of internal audit as a strategic ally, and should prompt the function to consider whether the organisation has a clear purpose, and whether risk management and related control processes support the organisation in achieving this purpose.
- **Principle 10**: The requirement for internal audit’s consolidated reporting uses the word ‘insights’ for the first time. Additional requirements are included regarding ongoing thematic reporting; providing insights on areas where internal audit has identified efficiencies, including removal of duplicative and/or redundant controls; and a requirement to provide an overall opinion on each of the areas of scope listed in **Principle 8**.

Next steps

Internal Audit functions must now incorporate the principles into their working practices. This will require firms to undertake a gap analysis against the revised standards to identify necessary changes.

Teams will need to consider any changes alongside the revised IIA’s Global Internal Audit Standards.

The CIIA combined Internal Audit Code of Practice (continued)

Key differences

- **Principle 11:** The annual report must support Board disclosures on risk management and material controls, highlighting any significant weaknesses, in line with the revised UK Corporate Governance Code.
- **Principle 14:** Requires that functions should coordinate with assurance providers on the organisation's key risks. We believe that this is a fantastic opportunity to optimise the holistic four lines model, through an enhanced organisation-wide assurance framework that gives clarity on the roles and remit of each assurance provider and control function, and effective coordination in the planning of risk coverage and reporting on key risks to the Board.
- **Principle 27:** The internal audit team should comprise internal auditors with a mix of backgrounds, skills and experiences who bring diversity of thought. The chief audit executive should recruit, retain and promote talent in accordance with the organisation's diversity, equity and inclusion ('DE&I') policies and applicable legislation. We fully support this new principle, but also recognise that it could be challenging to demonstrate conformance.
- **Principle 28:** Includes requirements to ensure that the right tools and technologies are in place to support the function's impact and effectiveness e.g. use of data analytics and artificial intelligence. This requirement would benefit from including the culture and behaviours needed to ensure these are implemented and embedded in ways that derive real value.
- **Principle 30:** Key Performance Indicators ('KPIs') must allow the audit committee to assess internal audit's value, impact, effectiveness and efficiency. We understand that this principle is intended to encourage functions to be more ambitious in defining how they measure their value and impact, beyond completion of annual audit plans. To do so is not straightforward, but can help internal audit to strategically focus on activities that add the greatest value to the business, to articulate the value they provide to the business and to justify the return on investment in the function.

Glossary of acronyms and abbreviations

AFM	Authorised Fund Manager
AI/ML/DL	Artificial Intelligence/Machine Learning/Deep Learning
ALCO	Asset and Liability Committee
AML	Anti-Money Laundering
AMLA	Anti Money Laundering Authority
AoV	Assessment of Value
APP	Authorised Push Payment
AWM	Asset and Wealth Management
BAU	Business As Usual
BCBS	Basel Committee on Banking Supervision
CBDC	Central Bank Digital Currency
BoE	Bank of England
CASS	Client Asset Sourcebook
CP	Consultation Paper
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CFTC	Commodity Futures Trading Commission
CDD	Customer Due Diligence
CRM	Contingent Reimbursement Model
CRR	Capital Requirements Regulation
CSDDD	Corporate Sustainability Due Diligence Directive
CSP	Cloud Service Provider
CSRD	Corporate Sustainability Reporting Directive
CVA	Credit Valuation Adjustment
CT	Consolidated Tape
CTP	Critical Third Party

D&I	Diversity and Inclusion
DE&I	Diversity, Equity and Inclusion
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
ECB	European Central Bank
EMR	Electronic Money Regulations
EMIR	European Market Infrastructure Regulation
ERP/EPM	Enterprise Resource Planning and Performance Management
ESAs	European Supervisory Authorities
ESMA	European Securities and Markets Authority
ESRS	European Sustainability Reporting Standards
ESG	Environment, Social and Corporate Governance
EU	European Union
FCA	Financial Conduct Authority
FPO	Financial Promotions Order
FinOps	Financial Operations
FRC	Financial Reporting Council
FRTB	Fundamental Review of the Trading Book
FS	Financial Services
FSMB/A	Financial Services and Markets Bill/Act
FTSE	Financial Times Stock Exchange
GDP	Gross Domestic Product
GI	General Insurance
HM	His Majesty
HM Treasury	His Majesty’s Treasury
IBS	Integrated Business Services

Glossary of acronyms and abbreviations (continued)

ICARA	Internal Capital Adequacy and Risk Assessment
IFPR	Investment Firms Prudential Regime
IFRS	International Financial Reporting Standards
IM(A)	Internal Model (Approach)
INED	Independent Non Executive Director
IRB(A)	Internal Ratings Based (Approach)
ISO	International Organisation for Standardisation
IST	Insurance Stress Test
KPIs	Key Performance Indicators
LATR	Liquid Assets Threshold Requirements
LDI	Liability Driven Investment
MI	Management Information
MiFID	Markets in Financial Instruments Directive
MiFIR	Markets in Financial Instruments Regulation
ML	Machine Learning
MRM	Model Risk Management
NFTs	Non-Fungible Tokens
OFAC	Office of Foreign Assets Control
OFTR	Own Funds Threshold Requirements
OECD	Organisation for Economic Co-operation and Development
PRA	Prudential Regulation Authority
PSD2	Payment Services Directive 2
PSP	Payment Service Provider
PSR	Payment Systems Regulator
PSRs	Payment Services Regulations
RAO	Regulated Activities Order

RM	Risk Margin
RWA	Risk Weighted Assets
SA	Standardised Approach
SARs	Suspicious Activity Reporting
SCA	Strong Customer Authentication
SCR	Solvency Capital Requirements
SDRs	Sustainability Disclosure Requirements
SEC	Securities and Exchange Commission
SFDR	Sustainable Finance Disclosure Regulation
SI	Statutory Instruments
SM&CR	Senior Managers and Certification Regime
SMF	Senior Management Function
SRS	Sustainability Reporting Standards
SUK	Solvency United Kingdom
TCFD	Taskforce on Climate-related Financial Disclosures
TCR	Transitional Capital Regime
TMTP	Transitional Measure on Technical Provisions
TPRM	Third Party Risk Management
TPR	The Pensions Regulator
UCITS	Undertakings for the Collective Investment in Transferable Securities
UK	United Kingdom
UN	United Nations
US	United States

Contact details

If you have any questions on any of the topics in this document, or would like a planning session, please reach out to your relationship contact or one of the following:

Nicole McManus
Internal Audit
Partner
+ 44 (0) 7989 950485
nicole.r.mcmanus@pwc.com

Steve Frizzell
Internal Audit
Partner
+44 (0) 7802 659053
steve.j.frizzell@pwc.com

Manjeet Gill
Internal Audit
Director
+44 (0) 7808 105658
manjeet.gill@pwc.com

Andrea Jaramillo
Internal Audit, Technology
Senior Manager
+44 (0) 7483 175621
andrea.l.jaramillo.toledo@pwc.com

Thank you

RITM0081803