The Risk Agenda for Assurance Functions 2026

Insurance & Asset and Wealth Management (I&AWM)
PwC
September 2025

In an era of constant motion; resilience, trust and assurance fuel confident reinvention.

Laura McSweeney

Director,
Insurance & Asset Wealth Management
Internal Audit Leader,
PwC UK

+44 (0) 7889 643707

laura.mcsweeney@pwc.com

The pace and interconnectedness of today's risks are reshaping how organisations grow, compete and are governed. PwC's Value in Motion study highlights how artificial intelligence (AI), climate risk and geopolitical shifts are reconfiguring value pools and creating new 'domains of growth,' underscoring the need for leaders to continually reinvent business, operating and energy models to stay ahead. The scale of change is significant: under a high-trust, high-adoption path, AI could materially lift global Gross Domestic Product (GDP) by 2035, while unchecked climate impacts could pull growth in the opposite direction.

The UK economic outlook adds further complexity. Persistent inflation in essentials such as food, clothing and transport, combined with fluctuating GDP figures, highlights a fragile recovery. Market expectations of near-term interest rate cuts have yet to ease uncertainty around growth, profitability and credit risk. A softening of the labour market, with job losses across labour intensive sectors is reshaping household spending and borrower capacity. For financial services firms, these dynamics increase the importance of resilient credit and liquidity models, effective customer support frameworks and robust scenario planning. At the same time, the UK Government's ten-year Financial Services Growth and Competitiveness Strategy, published in July 2025, sets out an ambitious agenda to secure the UK's position as the location of choice for investment, innovation and global growth.

Against this backdrop of accelerated change across regulation, technology and markets, Internal Audit will be pivotal in converting complexity into confidence, delivering forward-looking risk insight, agile assurance and constructive challenge so firms can innovate safely and grow.

PwC's Value in Motion study

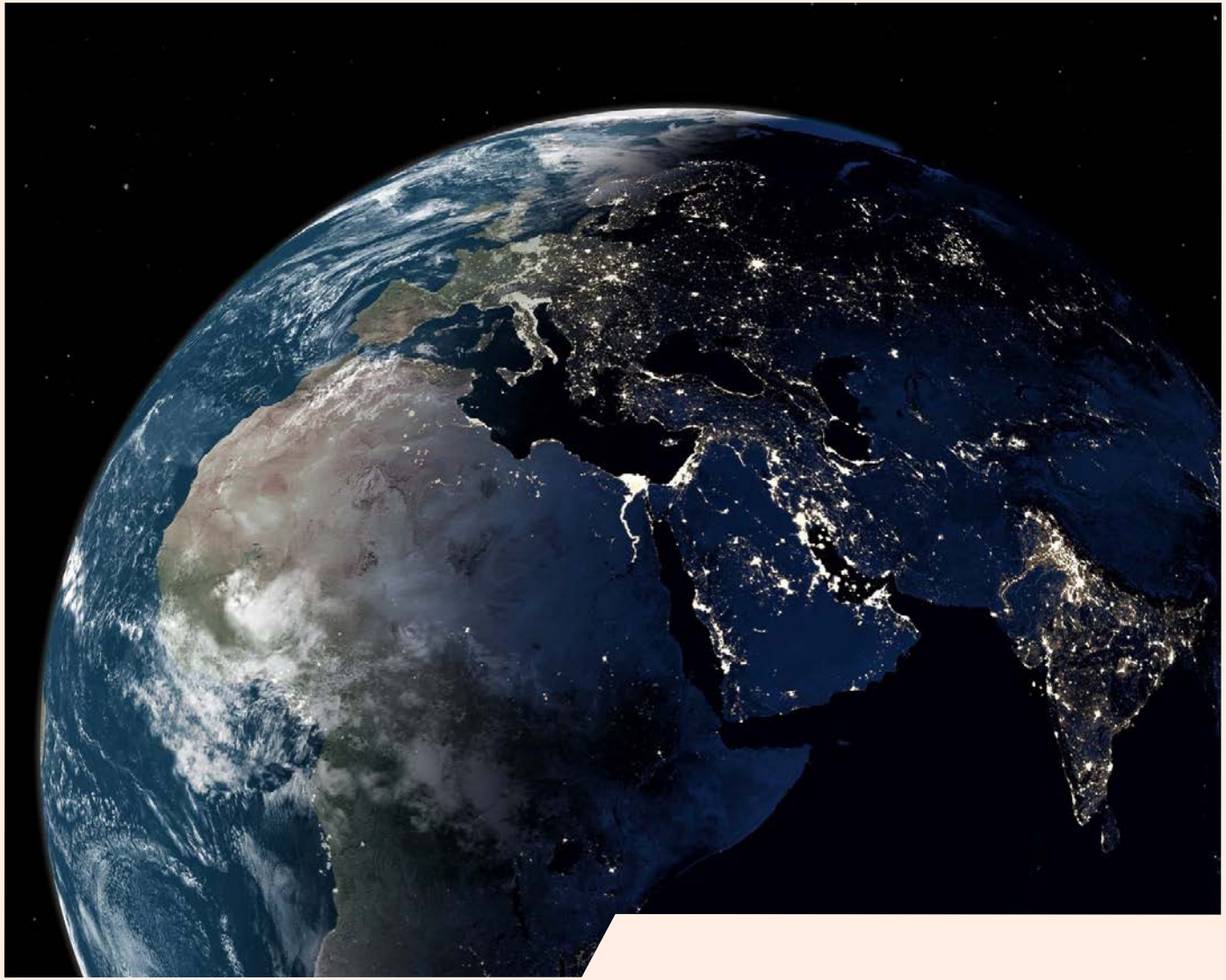
This year, our document covers the following areas:

- Macro Risk Landscape: This sets out the latest view on geopolitical uncertainty and the UK economic outlook.
- Regulatory Landscape: This includes the UK's Financial Services Strategy and the Leeds Reforms, alongside the Financial Conduct Authority (FCA)'s and Prudential Regulation Authority (PRA)'s 2025/26 priorities for the year ahead.
- Risk Hot Spots: We have curated a list of risk hot spots that are shaping boardroom discussions and impacting the financial services sector. These represent emerging and evolving areas of risk that assurance functions should be mindful of when setting priorities for the year ahead.
- Internal Audit Practices and Capabilities: This section includes what is front of mind for Chief Audit Executives. We share our point of view on the early experience on implementation of the Institute of Internal Auditor (IIA)'s Global Internal Audit Standards and Chartered Institute of Internal Auditors (CIIA) UK Code of Practice for IA which came into effect during 2025. Finally, we consider good practice in relation to the adoption of AI in IA.

We hope you find this a helpful document to guide planning for the year ahead and to spark meaningful conversations on risk and reinvention. If you would like 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.

Contents

Macro Risk Landscape



- Geopolitical uncertainty
- UK economic outlook

Geopolitical uncertainty

Summary

We continue to live in an era of geopolitical uncertainty. The systems and structures that have helped govern the global system in recent decades are weakening and changing. Global powers, responding to this changing environment, are competing for influence, and looking to new diplomatic, economic and security relationships. The level and pace of geopolitical shifts and shocks looks unlikely to lessen in the months ahead.

For businesses, changes in the geopolitical environment impact supply chains and production, regulatory and fiscal environments, global trade and tax norms, the movement of information, and the security of workforces, facilities and technology. In the coming year, organisations will be faced with the challenges emerging from three strategic themes:

Political Realignment	Globalism to Regionalism	The Decline of Multilateralism
01	02	03

What organisations should be doing

Against the backdrop of this continued volatility business leaders remain focused on adaptability and resilience:

Adaptability

As uncertainty increases, predicting the trajectory of international events will become increasingly difficult. Businesses need an effective monitoring and scenario analysis capability to provide early warning of emerging risks and opportunities. Agility in response is required to effectively mitigate risks.

Resilience

With the pace of change accelerating, businesses will not be able to plan for every scenario. Resilience means building the capacity to absorb shocks, maintain critical operations, and adapt quickly to new realities, ensuring the organisation can withstand disruption while positioning for recovery and growth.

Geopolitical uncertainty (continued)

Strategic themes

Looking to the year ahead, there are a number of strategic trends shaping the operating environment for UK and international firms.

Political Realignment

Many of the world's democracies are in transition following the 'year of elections'. Accompanying this is the growing popularity of far-right politics, increased political polarisation and a resulting rise in societal tensions.

Political realignments will be felt differently in different countries. This is most significant for businesses with an international footprint, where the political cultures of particularly Western democracies may be increasingly diverse. Organisations managing global workforces will need to navigate issues ranging from Diversity, Equity & Inclusion (DE&I) to immigration and regulation.

Political Transitions

2025 will be defined by political transitions as the anti-incumbent wave of 2024 elections reshapes governments worldwide. With opposition movements gaining influence and voter frustration fuelling polarisation, geopolitical uncertainty is set to rise.

The EU's (European Union) New Normal

Western Europe faces challenges from US tariffs, slow economic growth, and insecurity. Lasting solutions to these challenges will be extremely challenging.

Globalism to Regionalism

Multilateralism - the cooperation of multiple countries through international institutions and agreements - has long underpinned global diplomacy and trade. As approaches to multilateralism evolve, we are seeing a shift away from Western-led structures towards alternative models of influence. This is driving greater emphasis on regional alliances, national security priorities, protectionist trade barriers, and heightened competition over control of emerging technologies.

An increased focus on regionalism could impact global trade practices and encourage more localised models. Securing resilient and cost-effective supply chains will be increasingly challenging as organisations navigate complex regulatory environments, rising trade barriers and the weaponisation of trade as a geopolitical tool.

Trade re-orientation: Politically motivated and national security-related trade barriers are continuing to reshape the global trade environment. Divergence between the West and other global regions could result in incompatible trading and market regulations across all sectors, affecting, for example, data sharing.

Technology: Competition is at the forefront of technological innovation and will remain a key geopolitical driver. The focus on artificial intelligence, quantum computing and other advancements, including blockchain and digital assets, will lead to continuing competition across all aspects of innovation, from critical minerals to data, Intellectual Property (IP) and financial infrastructure. Control over tokenisation, central bank digital currencies (CBDCs) and digital payment systems is becoming increasingly linked to national security, digital sovereignty and future economic influence.

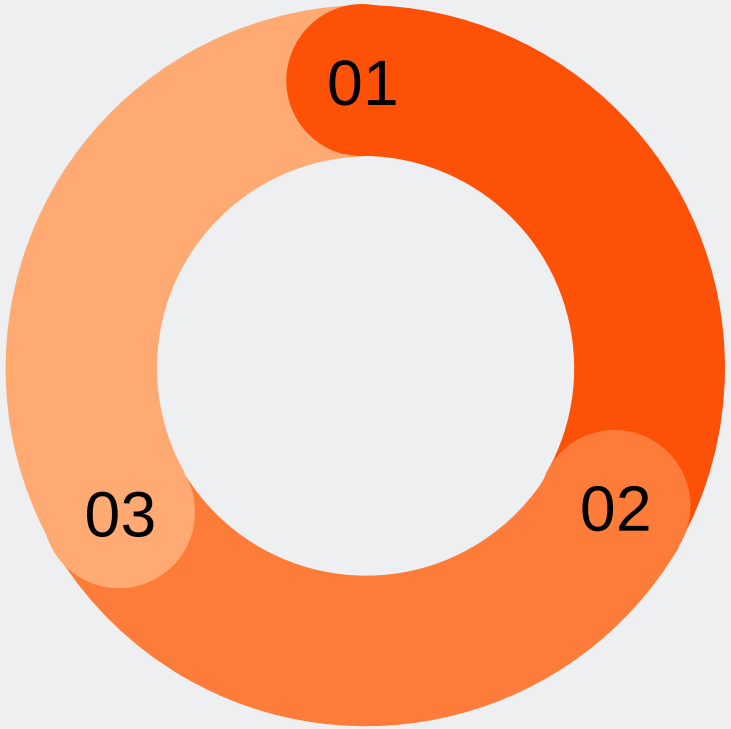
Changing international alignments: Emerging coalitions are gaining momentum and offer small and medium powers alternatives to a Western-led order. This could have implications for global security, as well as creating new norms and opportunities in global trade.

Geopolitical uncertainty (continued)

The Decline of Multilateralism

International institutions and norms that have long governed states' behaviour are weakening, leading to some states taking bolder unilateral actions with fewer consequences. Conflicts, cyber and physical sabotage attacks are continuing to proliferate as a result, and an increased sense of uncertainty and insecurity is driving defence spending globally.

The decline of multilateralism could lead to shifting global alliances, increased insecurity, and a disregard of international rules and conventions. Such changes can impact supply chains and production, regulatory and fiscal environments, global trade and tax norms, free movement of information, and the security of workforces, facilities and technology.



01 Europe-Russia Relations

Russian influence campaigns and 'grey zone' attacks such as cyber, sabotage, assassination attempts on defence industry executives, and attacks on undersea infrastructure will likely continue. This could undermine EU and North Atlantic Trade Organisation (NATO) unity, complicate the operating environment, and raise direct security threats.

02 Shifting Approaches to Defence

Rising geopolitical uncertainty, combined with US pressure on its allies to increase contributions, is likely to reshape approaches to defence spending. This could trigger action–reaction cycles, boosting opportunities for defence and security industries while reducing government funding available to other sectors.

03 Conflict Proliferation

As international norms break down, and the strength of international institutions weaken, there is a growing risk of interstate conflict. Even limited conflict events can impact security, operations, markets and supply, particularly if organisations are faced with multiple crises at once.

UK economic outlook

UK economic outlook: key themes and assurance implications

Inflation and Monetary Policy Trends

Recent data from the Office for National Statistics (ONS) shows persistent inflationary pressures, particularly in categories such as food, clothing, and transport. While market expectations point towards an interest rate cut in the near term, likely aimed at stimulating demand, uncertainty remains high.

For financial services organisations, a lower-rate environment could compress lending margins, affect pricing strategies for savings products, and shift investment portfolio performance. Internal audit functions should assess interest rate sensitivity across key areas of the business and test how well institutions are positioned to manage profitability in this changing landscape. Risk models may also require recalibration, particularly as high inflation combined with slowing growth revives the prospect of stagflation, prompting the need for targeted stress testing and scenario planning.

Commercial organisations face sustained input cost pressures, particularly in consumer-facing sectors such as retail, logistics, and consumer goods. These inflationary challenges, coupled with softening wage growth, are likely to squeeze margins and suppress consumer demand. Internal audit teams should consider reviewing pricing strategy governance, cost pass-through mechanisms, and inventory management to ensure resilience.

Public sector bodies must navigate heightened volatility in energy and transport prices, which may disrupt budget planning and forecasting accuracy. In addition, as the Bank of England adjusts its monetary policy stance, departments and regulators should closely monitor implications for debt servicing, benefit indexation, and funding allocations at the local authority level.

Gross Domestic Product (GDP) and Growth Outlook

According to the latest ONS figures, UK GDP contracted for a second consecutive month in May 2025. This slowdown follows a period of modest momentum earlier in the year and reflects declining output in key sectors such as automotive and pharmaceuticals.

For financial services organisations, weaker GDP growth translates into heightened credit risk and increased scrutiny over capital adequacy and liquidity buffers. Internal audit functions should test whether credit models are calibrated to reflect current macroeconomic risks and ensure that provisioning frameworks are responsive to a changing risk profile. This outlook also calls for strengthened governance over investment portfolios, including emerging exposures to tokenised assets and digital instruments, where market volatility and valuation methods may require additional scrutiny. Stress testing and scenario planning should also consider less liquid or novel assets held on or off-balance sheet.

Commercial organisations will need to reassess demand-side assumptions as growth slows. Lower consumer and corporate confidence may require businesses to revisit sales forecasts, pricing strategies, and cost control measures. Sectors like automotive and pharmaceuticals, which are experiencing contraction, should place renewed emphasis on supply chain resilience and export control effectiveness. Internal audit can add value by evaluating cost optimisation strategies, contract compliance, and supplier performance.

For public sector bodies, slowing economic activity may result in reduced tax receipts and put further pressure on public spending plans. Assurance functions should revisit fiscal planning assumptions, including contingency allocations and expenditure tracking. In addition, the economic environment may delay or reshape public programmes requiring closer oversight of risk registers, budget forecasts, and delivery milestones.

UK economic outlook (continued)

UK economic outlook: key themes and assurance implications (continued)

Labour Market Trends

June 2025 provisional figures show Pay As You Earn (PAYE) employment is down almost 180,000 over the past year. This looks like the second phase of a slowdown that began nearly two years ago, when firms pulled back on hiring. Now they're starting to cut roles.

Three labour-intensive sectors that are highly exposed to cost pressures are hospitality, wholesale and retail, and admin services which account for nearly two-thirds of the losses. AI may also be a factor, but our analysis indicates that a higher proportion of UK jobs are more likely to be augmented by AI rather than replaced by it. The question now is how far the job cutting goes, and what that means for household spending patterns. Job losses affect not just those who are out of work, but also others who are worried they might be next. This at least partly explains why the household savings ratio has more than doubled in recent years, even as wages are growing more slowly in real terms.

Looking ahead, much will depend on whether the government's recently announced capital spending plans can help rebuild confidence and support job growth in affected sectors.

In financial services sector, rising unemployment and strong wage growth may affect borrower capacity and increase demand for hardship support products. Internal audit teams should ensure credit models incorporate updated labour market assumptions and validate how customer assistance frameworks are being deployed. Treasury teams may also need to reassess their rate-related planning and hedging strategies, which audit can support through review of scenario planning and governance processes.

Commercial organisations will likely continue to focus on operational efficiency, including headcount reductions and contract renegotiation. Internal audit should evaluate whether staffing changes are aligned with business plans and whether labour compliance (e.g. IR35) is being maintained. Weaker demand may also necessitate adjustments to revenue forecasts, requiring assurance over forecasting processes and business planning.

Public sector bodies may experience rising demand for welfare services, with increased caseloads placing pressure on operational capacity. Internal audit teams should assess readiness and response planning, including how workforce constraints are being managed across critical public services. Additionally, greater coordination between fiscal and employment policy may be necessary, requiring assurance over data use, performance monitoring, and resource allocation

For further information on the UK Economic Outlook please our Economics webpage

Regulatory Landscape

- UK financial services strategy
- Leeds Reforms
- The FCA's focus for 2025/26
- The PRA focus for 2025/26
- Implications for financial services firms

UK financial services strategy

The UK Government published its ten-year Financial Services Growth and Competitiveness Strategy in July 2025, setting out the steps to deliver on its mission to be the location of choice for financial services (FS) firms to invest, innovate, grow and sell their services globally.

Financial Services Growth and Competitiveness Strategy

Delivering a competitive regulatory environment

Building a retail investment culture and delivering prosperity through UK capital markets

Embracing innovation and leveraging the UK's Fintech leadership

Harnessing the UK's global leadership in financial services

Setting the UK FS sector up with the skills and talent it needs

Delivery and Implementation

The Government calls for a deep, cohesive and ongoing partnership with business to deliver on the Strategy's vision.

The Government plans to set out progress against the Strategy's objectives on an annual basis against a range of success indicators, including net export share and growth, real wage growth in FS jobs, and net value of business finance raised.

Leeds Reforms

Alongside the launch of the UK's Financial Services Growth and Competitiveness Strategy, the Government, Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) published a series of updates, consultations and announcements known as the 'Leeds Reforms' to deliver on the Strategy's objectives.

01 Prudential

- Review of ring-fencing regime
- PRA confirms delay of Fundamental Review of the Trading Book (FRTB) and Internal Model Approach (IMA) implementation to 1 Jan 2028
- PRA to raise minimum requirements for own funds and eligible liabilities (MREL) thresholds
- PRA to explore greater flexibility on internal ratings-based (IRB) model permissions

02 Capital Markets

- FCA final rules for Public Offers and Admissions to Trading Regime (POATRs) and Public Offer Platform (POP) regime
- FCA to continue review and reform of MiFID, European Market Infrastructure Regulation (EMIR) and Benchmarks Regulation (BMR)

03 SM&CR

- FCA and PRA Phase 1 consultation e.g. changes to 12-week rule
- His Majesty Treasury (HMT) Phase 2 consultation on legislative changes e.g. removing Certification Regime from statute

04 Sustainability

- Green Taxonomy to be dropped
- HMT to lay legislation to bring ESG ratings providers into scope by end 2025 and consult on UK Sustainability Reporting Standards.

05 Financial Ombudsman Service (FOS)

- FCA/FOS consultation on major reforms, including on FCA referrals, adapting 'fair & reasonable test, 10-year limit on complaints

06 Wholesale Financial Markets Digital Strategy

- 10-year strategy to optimise outdated systems, transform markets via technology, & position UK as a global digital leader

07 Targeted Support

- Confirm targeted support to be operational by 2026 ISA season
- Long term asset funds (LTAF) to be held in stocks & shares ISAs from 2026

08 Insurance

- PRA and FCA to consult on captive insurance regime in summer 2026
- Government consultation on UK insurance linked securities offer

09 National Payments Vision

- Bank of England (BoE) announced reset to UK retail payments infrastructure.
- Full strategy to be published in autumn 2025

The FCA's focus for 2025/26

The FCA outlines how it will deliver on its strategic priorities and enhance the integrity, innovation and competitiveness of UK financial services. Initiatives are structured around the regulator's four strategic priorities:

FCA 2025-30 Strategy

A more efficient and effective regulator

- Streamlining regulatory interactions to reduce the burden on firms.
- Enhancing supervisory and intelligence capabilities.
- Strengthening detection and response to harm.

Supporting growth

- Unlocking capital investment and liquidity.
- Accelerating digital innovation to improve productivity.
- Reducing the regulatory burden.
- Providing certainty and predictability.
- Enabling firms to start up and grow.
- Promoting UK exports and inward investment.

Helping consumers navigate financial lives

- Promote the development of innovative solutions to enhance consumer resilience.
- Continue efforts aimed at long-term financial wellbeing and improved experiences engaging with financial services.

Fighting financial crime

- Strengthen approach to financial crime.
- Enhance collaboration and data sharing with partners to increase efforts to disrupt organised crime and prevent money laundering.

Examples of relevant work streams (some may be relevant for multiple priorities)

- Reduce regulatory reporting burden.
- Digitise and simplify authorisations process.
- Target market engagement on areas where harm is the greatest.
- Take a more flexible supervisory approach.
- Be more transparent, accountable and aligned to strategic objectives.

- Progress pension reform.
- Embrace digital first approach as a regulator.
- Partner with Government and others to create a system that strengthens the UK's global competitiveness.
- Streamline rules, guidance materials and wider communications.
- Review Senior Managers and Certification Regime (SM&CR).

- Consumer Duty and vulnerable customers.
- Advice guidance boundary review.
- Pensions dashboard.
- Introduce regulatory framework on the long-term value of pension products.
- Support delivery of measures in the expected Pensions Bill.

- Build a new data-led detection capability
- Focus on proactive assessments of anti-money laundering systems and controls for high-risk firms
- Provide continued support for development of new innovation and technology (e.g. through RegTech firms)

The PRA's focus for 2025/26

The Prudential Regulation Authority (PRA)'s priorities for 2025/26 reflect an evolution of its key focus areas from previous years, with a sustained focus on delivering against its secondary objective for competitiveness and growth. From a supervisory perspective, the PRA's focus continues to remain on critical areas including governance, risk management, controls, and operational and cyber resilience.

PRA 2025/26 Strategic Priorities

01 **Maintain and ensure the safety and soundness of the banking and insurance sectors and ensure continuing resilience**

02 **Be at the forefront of identifying new and emerging risks, and developing international policy**

03 **Support competitive, dynamic and innovative markets, alongside facilitating international competitiveness and growth**

04 **Run an inclusive, efficient, and responsive regulator within the central bank**

Supervisory priorities – 2025

Risk management capabilities

- The PRA notes that firms continue to vary in their ability to proactively identify, monitor and manage emerging and novel risks, including from geopolitical and technological developments.
- The PRA emphasises that firms' senior management and Boards should ensure robust governance, risk management and controls frameworks are in place – ensuring these are adaptive and resilient, leveraging stress and scenario analyses to inform risk management, strategy, and business planning.

Prudential reforms

- The PRA is continuing with its focus on prudential reforms including through the implementation of Basel 3.1 and Solvency UK reforms.
- Following the implementation of all Solvency UK reforms in 2024, this year the PRA will prioritise ensuring that these reforms are embedded.
- Additionally, the PRA plans to continue to collaborate with the government and other stakeholders to identify steps to help insurers fully benefit from the reforms, including engaging with the National Wealth Fund and creating a Matching Adjustment Investment Accelerator.

Operational resilience, cyber, and ICT risks

- Firms were required to meet the PRA's operational resilience requirements by March 2025, the PRA's supervisory focus will now be on ensuring the regime is fully embedded.
- To further enhance the sector's cyber resilience capabilities, the PRA plans to begin consulting with the FCA in H2 2025 on policy related to the management of Information and Communication Technology (ICT) and cyber risks.

Financial risks arising from climate change

- The PRA has proposed updates to its 2019 supervisory expectations (SS3/19) on managing climate-related risks, set out in Consultation Paper CP10/25 published on 30 April 2025. The proposals mark a clear step up in regulatory expectations and would require firms to embed climate risks into their strategy, align governance and decision-making processes, and strengthen climate risk frameworks through more robust scenario analysis.

Implications for financial services firms

The Financial Services Growth and Competitiveness Strategy, coupled with the breadth and depth of ongoing regulatory reformsreinforces the Government's desire to move the regulatory debate into a new phase and rebalance the level of risk in the system.

The impact of the Government's intensified focus on growth and competitiveness will have significant implications for financial services firms, including for firms' strategies, business models, risk appetite and risk management.

Outcomes-based regulation

A continued trend towards outcomes-based regulation will place greater emphasis on firms' evolving their compliance and risk management processes to proactively understand and gain comfort in the outcomes they are delivering for their customers/clients.

01

New opportunities

Streamlined or more tailored regulatory requirements may provide strategic opportunities for firms to reconsider their risk appetite, enhance their product or service offering, access new markets, and leverage regulatory agility to gain competitive advantage.

02

Technology

Authorities are taking action to ensure the regulatory framework supports innovation, including on digital assets, stablecoins, tokenisation and AI. Firms should consider opportunities to harness technology development, both in enhancing their products/services and supporting efficient and resilient systems and processes.

03

Resilience

Despite the Government's mission to support growth and competitiveness, Financial Conduct Authority and Prudential Regulation Authority supervision will continue to focus on ensuring that firms have appropriate risk management, systems, controls and resilience that is proportionate for their business and responsive to evolving economic and market conditions.

04

Risk Hot Spots

Contents

AI – Governance of Agentic and Generative AI

Artificial Intelligence (AI) systems with agentic capabilities (which make decisions and take actions to achieve goals), and generative capabilities (which create new content such as text, code, or images), are introducing complex governance risks that many organisations are not yet prepared to manage.

Governing Agentic and Generative AI: Managing autonomy, ethics, and accountability in intelligent systems

Agentic and Generative AI systems are transforming how organisations operate, innovate, and engage with stakeholders. These advanced AI systems are capable of autonomously making decisions, generating content, and executing tasks in complex enterprise settings without constant human intervention. As their capabilities grow, the boundary between human-led decisions and AI-driven actions becomes increasingly blurred.

Traditional governance models, designed for static and rule-based technologies, are not equipped to handle the dynamic nature of these new systems. Emerging risks include loss of control, misalignment with human intent, hallucinations or incorrect outputs, and unintended consequences that scale rapidly. The lack of visibility into how generative models work also raises concerns around explainability, ethical use, and regulatory compliance.

Governance of these technologies must evolve to include a broader view of risk, oversight, and assurance. Regulatory developments, such as the EU AI Act and the UK's emerging AI governance principles, signal a shift towards stronger expectations for transparency, accountability, and safe deployment. Organisations need to act now to build effective governance frameworks that enable innovation while managing the risks associated with intelligent and autonomous systems.

Key considerations for organisations

As organisations scale the use of AI, especially agentic and generative capabilities, they must address business-critical risks including loss of control, reputational damage, regulatory non-compliance, and ethical misalignment.

Design AI-specific risk frameworks that account for autonomy, decision-making thresholds, safe failure modes, and alignment with human intent.

Implement explainability and transparency practices to ensure that users and stakeholders understand how outputs are generated, and decisions are made.

Clarify decision boundaries by mapping out where AI can operate independently and where human judgment must intervene, including escalation protocols for deviations.

Continuously evaluate training data and model performance to detect bias, drift, and harmful content, and ensure responsible data sourcing and documentation.

Prepare for compliance with fast-evolving AI regulations, including sector-specific expectations from regulators such as the Financial Conduct Authority (FCA), Information Commissioner's Office (ICO), and National Health Service (NHS).

Embed AI governance within existing enterprise risk, control, and compliance frameworks to ensure consistency and avoid siloed approaches.

Promote a culture of responsible AI use, supported by values-based principles and cross-functional collaboration across data, risk, legal, compliance, and assurance teams.

AI – Governance of Agentic and Generative AI (continued)

Understanding Agency in Artificial Intelligence (AI): Use case complexity, risk, and enterprise readiness

Understanding the path to Agentic AI and enterprise transformation

As organisations adopt more advanced AI capabilities, they are progressing beyond simple embedded applications toward complex, adaptive, and agentic systems. This shift involves not only increased technological sophistication but also a step-change in how AI systems are designed, governed, and integrated into enterprise operations.

Agentic systems are defined by their ability to make decisions and act independently in pursuit of goals. The level of agency depends not just on the AI model itself but also on the complexity and openness of the tasks assigned. As firms move toward these more autonomous systems, they must address heightened risks around control, assurance, and alignment with strategic objectives.

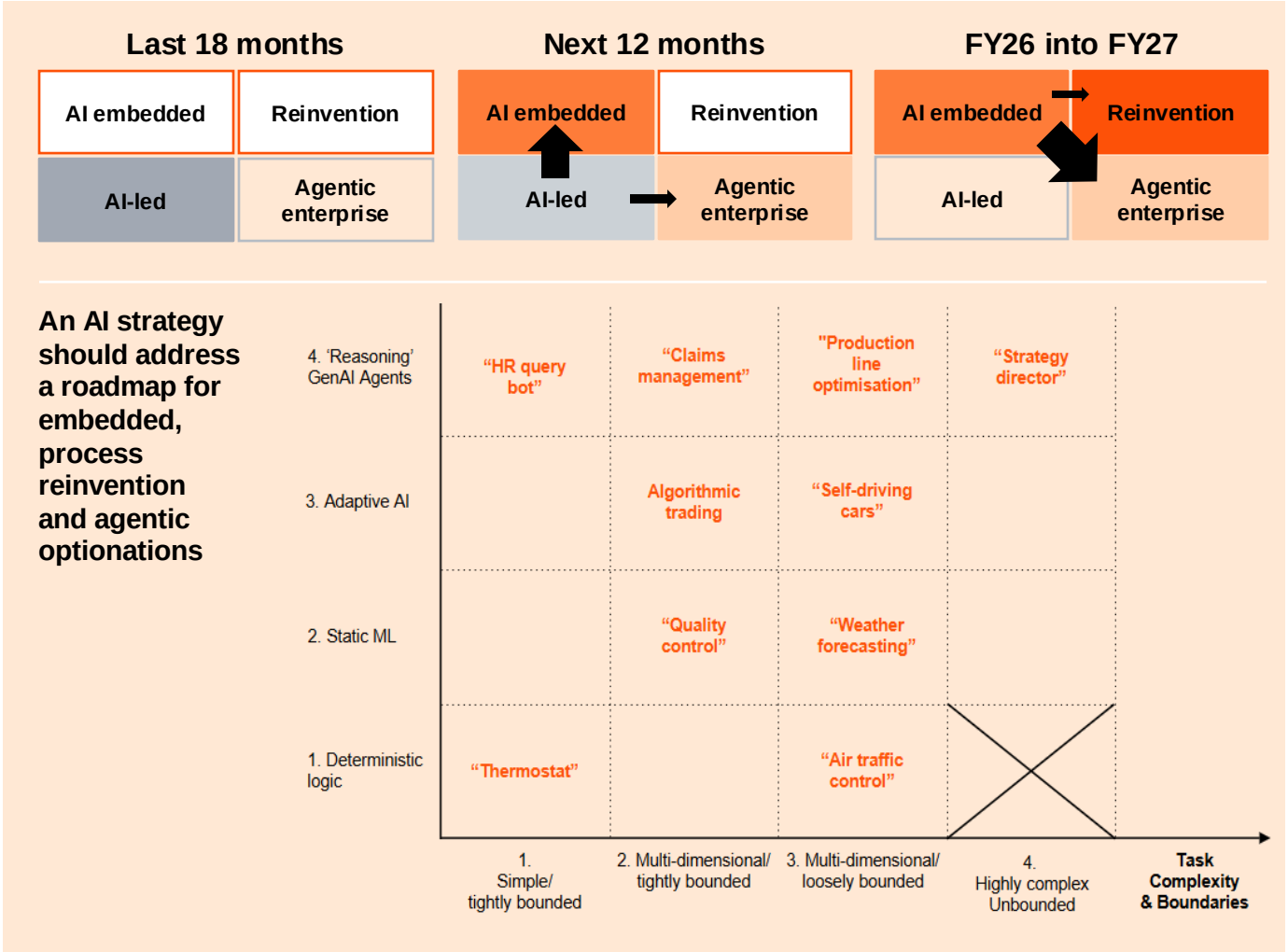
A clear roadmap is needed to support this evolution, one that connects technical capability with organisational transformation. This includes planning for AI embedded solutions, process reinvention, and eventually, the emergence of the agentic enterprise.

Use case positioning shows how autonomy and task complexity increase risk

The diagram to the bottom-right illustrates how different AI use cases vary in autonomy and task complexity, helping to highlight where stronger governance and assurance are most needed.

Systems like thermostats are simple and rule based, while agentic examples like strategy director or production optimisation operate independently in dynamic environments.

As systems move up and to the right, they require stronger governance, clearer accountability, and more advanced assurance frameworks tailored to dynamic and autonomous behaviour.



AI – Governance of Agentic and Generative AI (continued)

Internal Audit focus areas

01

Governance and accountability

- Review governance structures, escalation protocols, and board-level oversight.
- Assess integration of AI risks into the enterprise risk taxonomy.
- Evaluate assurance arrangements for third-party AI tools, models, and APIs.

02

Model and data lifecycle management

- Review development and data lifecycle practices (version control, retraining, validation, model drift).
- Confirm audit trails, logs, and documentation exist for traceability and explainability.

03

Monitoring and resilience

- Test monitoring controls, feedback loops, and anomaly detection protocols.
- Validate disaster recovery and continuity plans for AI systems.

04

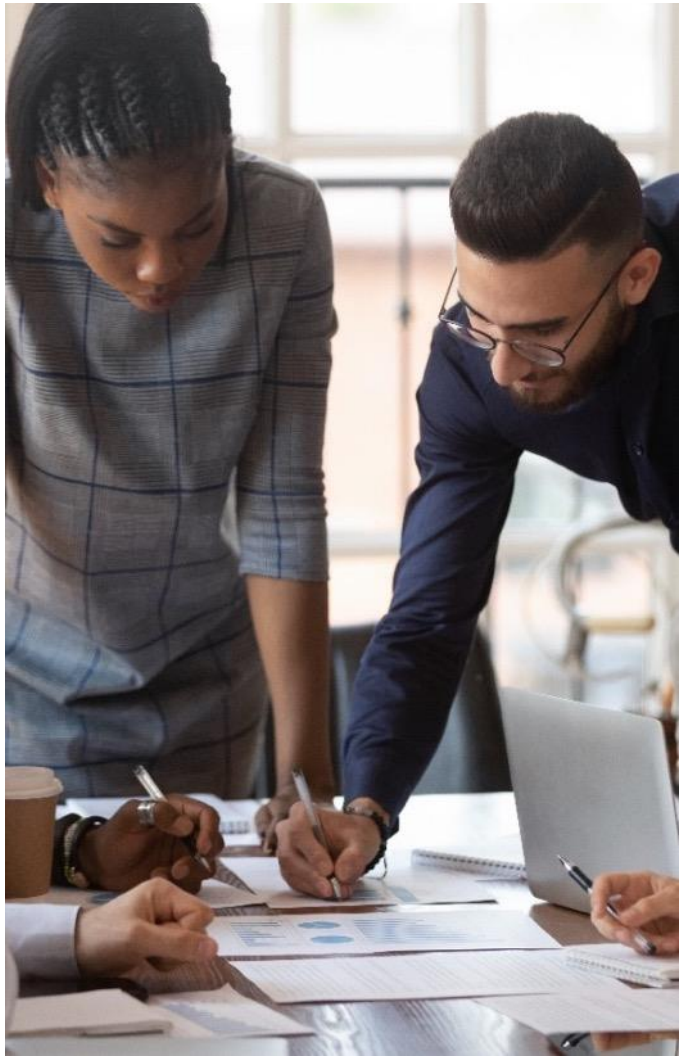
Ethics and security

- Examine how fairness, transparency, and accountability are embedded in AI design and deployment.
- Evaluate security measures protecting AI data and models from manipulation or hacking.

05

People and strategy

- Investigate training programmes for users and employees on AI risks and functionality.
- Review the organisation's AI strategy to ensure alignment with business objectives and long-term value.



AI – AI Talent and Skills Gap (AI enabled workforce)

Despite rapid adoption of Artificial Intelligence (AI) across business functions, most organisations lack the skills and workforce models needed to deploy AI responsibly and effectively at scale, exposing them to operational, ethical, and regulatory risks.

Governing AI talent and the skills gap: enabling a responsible, adaptive, and AI literate workforce

Organisations are investing heavily in AI, but their people and operating models are not always prepared to keep pace. Across business functions, employees are increasingly interacting with AI tools and relying on AI generated outputs to support decisions. This shift is not limited to data scientists or engineers. It includes assurance professionals, operational teams, legal and compliance functions, and executives using AI to drive strategy.

The skills gap is broader than just technical knowledge. It includes awareness of AI risks, responsible use, ethical boundaries, and the ability to interpret AI supported insights. Without this understanding embedded across the workforce, organisations face increased exposure to mistakes, misuse, reputational damage, and regulatory non-compliance.

To safely scale AI adoption, firms must align workforce planning with AI maturity, establish role clarity and guidance, and embed capability building across their governance, control, and assurance environments.

Refer to the link below for PwC's 2025 Global AI Jobs Barometer, which explores AI's impact on jobs, skills, and wages. The report provides valuable insight into how AI is shaping labour markets, redefining skills requirements, and influencing productivity.

PwC's 2025 Global AI Jobs Barometer

Key considerations for firms

To realise the benefits of AI safely and effectively, firms must ensure their workforce is equipped with the right skills, governance clarity, and cultural readiness to support responsible adoption across all areas of the business.

Identify the AI related skills and responsibilities needed across leadership, risk, operations, assurance, and frontline roles.

Develop and embed an AI skills strategy that promotes awareness, critical thinking, and ethical use across all business units.

Establish clear rules and oversight around AI tool usage, including who can use them, for what purposes, and under what control conditions.

Build internal understanding of core AI concepts such as model limitations, explainability, data quality, and the need for human judgment.

Invest in upskilling programmes, cross functional teaming, and partnerships that expand organisational capability beyond technical specialists.

Implement acceptable use policies for public or third-party AI platforms and ensure these are actively communicated, governed, and enforced.

Promote a responsible innovation culture where employees are encouraged to experiment with AI in a controlled and supported environment.

Align learning and development with emerging regulatory expectations and integrate it into performance, compliance, and change programmes.

AI Talent and Skills Gap (AI enabled workforce) (continued)

Internal Audit focus areas

01

Roles and responsibilities

- Evaluate whether critical roles requiring AI fluency or responsible usage awareness are defined, and whether skills gaps are identified and tracked.
- Review workforce and resourcing plans to confirm they reflect the firm's AI objectives and whether assurance functions are adapting their skills accordingly.

02

Governance and access controls

- Assess governance over access to and use of AI tools, ensuring control conditions, permissions, and monitoring are clearly defined.
- Test whether acceptable use policies for AI are clearly communicated, embedded into daily practice, and applied consistently in regulated or sensitive areas.

03

Escalation and issue management

- Determine if employees understand how to escalate concerns about AI outputs, misuse, or unintended consequences, and whether escalation channels are effective.

04

Training and awareness

- Review the availability, content, and coverage of AI risk and ethics training across all organisational levels.
- Assess how cross-functional collaboration supports safe and effective use of AI tools across business units and lines of defence.

Cyber – Identity and Access Management

Identity attackers are increasingly using compromised identities as an entry way into organisations to exfiltrate data. Robust identity management is the key to defend against modern identity threats such as phishing, credential stuffing, and social engineering.

Attacks on identities are increasingly becoming the primary cause of significant cyber breaches. The conventional perimeter is disappearing, and identity has emerged as the new perimeter. In increasingly hybrid and cloud-native environments users are accessing systems from multiple locations, devices, and networks. As such infrastructure is increasingly virtualised with third parties and customers connecting via platforms and portals.

Identity is complex across sectors where potentially thousands of internal users and extensive third parties have access and where legacy systems do not integrate well with modern systems. Identity is not just a tech problem, it is a governance problem as well, and many organisations struggle with orphaned accounts, overprivileged roles, lack of Joiner-Mover-Leaver enforcement and minimum identity assurance for non-human accounts.

Key considerations for firms

In the FS sector alone, 93% of organisations experienced at least two identity-based attacks in the last 12 months. As a result, increased investment in identity security is more pertinent than ever, especially if there has been a lack of investment previously. Organisations should look at leveraging modern identity controls from the outset to bolster identity security.

Uplifting security programmes to defend against the compromise of identities can be done by implementing a zero-trust access principle to modernise identity and access controls. Identity controls also need to be hardened against evolving threats with specific training rolled out around new social engineering threats and dedicated training for help desk staff.

80% of data breaches stem from compromised identities with third-party access which is considered an increasingly common identity governance challenge for organisations. The evolution in threat requires an evolution in strategy to move from compliance-led to more threat-led.

Building threat focused identity capabilities can be done by focusing on:

- Continuous identity security posture and exposure management
- Identity threat detection and response
- Just in time and just enough access
- Risk based access controls

Threat management tooling should also be extended to cover identity by deploying identity specific threat detection and response tooling and expanding red and purple teaming to cover identity-based attacks and social engineering.

Cyber – Identity and Access Management (continued)

Internal Audit focus areas

01
Governance and strategy

- Assess whether Identity and Access Management (IAM) governance structures, roles, and accountabilities are clearly defined and aligned to the organisation's overall security strategy and risk appetite.
- Review Board and senior management oversight, including reporting mechanisms, KPIs/KRIs, and escalation protocols.
- Evaluate whether IAM policies, standards, and procedures are up-to-date, approved, and consistently implemented across the organisation.

02
User access provisioning and lifecycle management

- Test the adequacy and timeliness of access provisioning, modification, and de-provisioning processes (e.g., joiners, movers, leavers).
- Validate segregation of duties controls to ensure access conflicts are identified and appropriately mitigated.
- Confirm whether privileged access management (PAM) processes are in place and effective.

03
Authentication and access controls

- Evaluate the use and effectiveness of multi-factor authentication (MFA), password standards, and session management.
- Review system-enforced access controls and role-based access models to confirm alignment with the principle of least privilege.
- Test access restrictions to critical systems, applications, and sensitive data, including cloud and third-party hosted environments.

04
Monitoring, logging, and incident management

- Review the design and effectiveness of monitoring controls, including logging, alerting, and anomaly detection for unusual access activity.
- Assess whether escalation and incident response processes for IAM-related breaches are defined, tested, and aligned to broader operational resilience frameworks.
- Validate the adequacy of periodic user access reviews, certification processes, and reconciliations across business critical systems.

05
Regulatory and compliance alignment

- Evaluate alignment of IAM controls with regulatory requirements (e.g., PRA/FCA, DORA, ISO 27001, NIST).
- Confirm that IAM practices are adequate to support audit trails, accountability, and regulatory reporting expectations.

Cyber – Response and Recovery

Response and recovery is a crucial part of cyber security to ensure business continuity and to minimise damage from security breaches. Only 2% have implemented cyber resilience actions across their organisation in all areas surveyed.

Response: Prompt and decisive actions are crucial when a cyber breach occurs. Initially, it's imperative to quickly detect the incident, ensuring anomalies are recognised and reported immediately. Following detection, the swift isolation of compromised systems is essential to halt the attack's progression and prevent the threat from spreading further, allowing the response team to focus on mitigation strategies without incurring additional damages.

Recovery: Preserving evidence is vital during the recovery process. This involves capturing system logs, taking snapshots, and rigorously documenting all actions taken throughout the incident response. Such measures not only support investigations but also enhance the organisation's ability to bolster future defences. Equally important is the restoration of systems, data, and services to their original state safely and securely. Resilience in recovery processes is pivotal for maintaining operational integrity and rebuilding stakeholder confidence.

In the past 12 months, cyber incidents such as those targeting a prominent UK retailer and attributed to Scattered Spider have had considerable repercussions. These attacks led to significant operational disruptions, including an inability to process online orders and shortages on store shelves. Additionally, they caused a sharp decline in share prices and eroded customer trust, highlighting the profound impact of cyber threats on businesses. The necessity for robust response and recovery strategies has never been more apparent, as organisations strive to protect their assets and uphold their reputations in the face of increasingly sophisticated threats.

Key considerations for firms

There are time sensitive actions that should be taken in the first moments of a ransomware incident, including:

- Embarking on immediate action to limit the damage (e.g. disconnecting critical systems).
- Appointing / consulting with specialist third parties including:
  - External Legal Counsel; and
  - Incident Response (IR) provider(s).
- Invoking a command-and-control structure.
- Deciding whether to operate under legal privilege.
- Identifying safe channels for communications.

Organisations are often not prepared for the rapid and complex response required, with complex IT environments and often unclear information about critical systems restoration can present a significant challenge.

Organisations must engage constructively with regulators and ensure they understand the obligations in managing the response potentially across multiple jurisdictions.

Sustaining business operations while IT systems are being recovered presents a challenge, often necessitating the continuation of business activities without IT support, potentially lasting several weeks or longer.

In the initial stages of a ransomware incident, timely actions are crucial. Organisations should ask critical questions like:

- Have we identified and mapped out essential business processes?
- Do we have immutable backups in place, and have we tested our ability to restore from them?
- Are there contingency plans for vital business operations?
- Can we restore our most privileged assets and accounts, including identity management systems like Entra and IAM services, if needed?

Further considerations include in the following:

- Have we established clear communication channels for crisis management?
- Do we have an incident response team ready to engage immediately?
- Are the security patches and system updates current?
- Can we quantify the potential financial and reputational impacts?

These questions help assess readiness and resilience in facing IT risks and ensuring business continuity.

Cyber – Response and Recovery (continued)

Internal Audit focus areas

01
Governance and Oversight

- Assess clarity of roles, responsibilities, escalation protocols, and Board/ executive oversight during cyber events.
- Assess how cyber response and recovery arrangements incorporate third parties, suppliers, and outsourced services.

02
Incident detection and response

- Review monitoring, detection, and response processes, including timeliness and effectiveness of escalation.

03
Recovery and continuity

- Evaluate recovery strategies, playbooks, and restoration plans for critical systems and data to confirm alignment with resilience requirements.

04
Testing and exercises

- Validate the adequacy and frequency of cyber incident simulations, crisis management exercises, and lessons-learned integration.

05
Regulatory and reporting compliance

- Review alignment with regulatory requirements (e.g., PRA/FCA, DORA, NIS2) for incident reporting, notification timelines, and recovery expectations.

Cyber – Threats emerging from AI

Advancements in Artificial Intelligence (AI) have led to exploitation shifts and a widening gap between development and detection capabilities.

In the world of cyber threat actors, automation is not a new concept. Whether it is automating the scanning of vulnerable internet facing devices or scripting functions that easily propagate ransomware across a network, the modern threat has evolved to be an automated attack system. This notion raises the question of how will new AI technologies change the way attackers conduct their malicious activities, which in many cases, are already relying less on human-input.

The degree to which AI, particularly GenAI, technologies have advanced over the past year is significant and indicative of an ongoing race among those seeking to develop, invest in, embrace, operationalise, and exploit these solutions. This advancement, however, has caused a widening gap between these technologies and the technologies developed to detect AI-generated content and media.

Threat actors have, and will, continue to capitalise on this widening gap, exploiting AI solutions and developments to enhance their operations and impact on victims. By leveraging AI, threat actors are able to enhance their attacks making them faster, more sophisticated and more targeted than ever before. This targeting at scale underpins the importance for continuous threat exposure management to proactively identify, assess and mitigate risk and highlights the need for organisations to prioritise robust and timely vulnerability management.

Key considerations for firms

The potential use cases for a threat actor leveraging AI could theoretically be endless, however, there are several areas that stand out and have potential for improving the success of attacks:

- Social engineering and access operations;
- Targeting at scale;
- Identification or processing of targets; and
- Attack playbooks.

As the threat landscape is constantly evolving and with the advancements in AI contributing to that it is key that organisations:

- Have a dynamic and proactive approach to identifying and responding to new attack vectors;
- Maintain robust supply chain and third-party management;
- Have clear accountability and responsibility of AI and machine learning security within the organisation;
- Ensure security is factored in any decisions on the adoption of AI tools;
- As AI provides increased capabilities in reconnaisance and social engineering it is imperative the training and awareness programmes of organisations are adapted to address this accordingly; and
- AI should also be leveraged to improve the detection and triage of cyber attacks, helping to identify malicious emails and phishing campaigns.

The following exploitation trends have also been identified:

Threat actors using AI tools to conduct reconnaissance activities against a target organisation, its operations and employees, as well as the broader industry, for use in follow-on activities, such as financially motivated attacks, exploitation of identified vulnerabilities, disinformation campaigns, and social engineering against key roles.

Threat actors targeting AI tools that may be adopted by an organisation, such as customer-facing chatbots or internal tools used by the organisation's employees, to steal sensitive information (e.g., user inputs involving proprietary information, biometrics, user behaviour analytics, etc.).

The use of deepfake video content and AI generated voice-based technology pose detection challenges. Voice or audio is one of the most important channels of human communication, and GenAI developments in this space therefore have potentially significant ramifications for security. There have already been numerous documented examples of where malicious threat actors have sought to exploit this type of content generation. Application to date has largely although not exclusively been financially motivated, but the potential application of this technology is much wider, including for espionage or disinformation purposes.

Cyber – Threats emerging from AI (continued)

Internal Audit focus areas

01
Governance and risk assessment

- Assess how AI-related cyber risks are identified, evaluated, and integrated into the enterprise risk taxonomy and cyber risk appetite.

02
AI system security

- Evaluate safeguards protecting AI models, data, and algorithms from manipulation, adversarial attacks, or unauthorised access.

03
Threat detection and monitoring

- Review controls for detecting and responding to AI-enabled attacks, including anomaly detection, behavioural analytics, and incident escalation processes

04
Third-party and supply chain risks

- Verify oversight of AI-related risks introduced through vendors, cloud providers, and third-party tools

05
Training and awareness

- Test training and awareness programmes to ensure employees can recognise AI-enabled threats (e.g., deepfake fraud, generative phishing) and respond appropriately.

06
Regulatory and ethical alignment

- Validate alignment with emerging regulatory standards and ethical guidelines on AI use in cyber defence and resilience.

Operational Resilience

Operational resilience remains a top priority, especially as financial services firms are subject to increasingly complex, sophisticated and evolving risks. While implementation deadlines have elapsed for financial services firms across multiple regions, regulators particularly in the UK, expect firms to treat resilience as an evolving capability to prevent, respond, learn and adapt to disruption.

By July 2025, 70% of the top 20 largest countries (by GDP) have released / subscribed to a set of resilience rules / guidelines. By Q3 2025, a large majority of these rules will be in force, including those prescribed by the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) in the UK.

The PRA and FCA have stated that the March 2025 implementation deadline for UK firms in scope "should not be seen as the destination for operational resilience, rather the start of an ongoing requirement to maintain, manage and keep building resilience".

For financial services, given where the industry is in the regulatory cycle on resilience (i.e. post deadline) it is important that firms can continue to focus on maturing their resilience capabilities as processes, firm strategies and markets all develop dynamically in response to the external threat landscape and market structure.

IA teams will need to shift their approach to providing assurance on resilience to align with its dynamic nature.

Key considerations for firms

In the post-deadline era, firms should consider the following:

Evolving regulatory expectations:

In the UK, there are evolving regulatory expectations which include new rules for third-party resilience, cyber resilience, physical climate-related risks, and the transition to T+11. Firms need to understand the impacts of these changes to their resilience capabilities, and gain assurance on how they have met these considerations.

Embedding resilience within existing frameworks (i.e. risk):

As firms become more confident in their resilience programmes, they need to create alignment to gain the benefits of a more holistic risk and resilience approach. This is becoming more of a focus.

Consider workforce availability and skills gaps:

Firms must ensure that their internal capabilities can respond dynamically to evolving internal and external risks.

Managing applicable cross-border requirements:

Several resilience regulations/guidelines are in force, and firms in scope are generally aligning with the existing rules. Firms operating across multiple jurisdictions have an opportunity to evolve their resilience capabilities by adopting lessons from other jurisdictions where applicable, especially where they face similar risks and threats/share similar value chains. The level of integration could be proportionate to the firm's risk environment, business strategy, and level of regulatory scrutiny.

Continually evolve testing to understand the impact of internal and external changes on the resilience of important services:

The FCA in the UK has discussed how firms can increase the sophistication of their testing programmes through integrated testing programmes and threat-led penetration testing. Other global regulators have introduced unique requirements within their rules, e.g. Monetary Authority of Singapore (MAS) which requires firms in scope to validate the efficacy of remedial actions identified in previous tests, and in subsequent tests.

Operational Resilience (continued)

Internal Audit focus areas

01
Governance and oversight

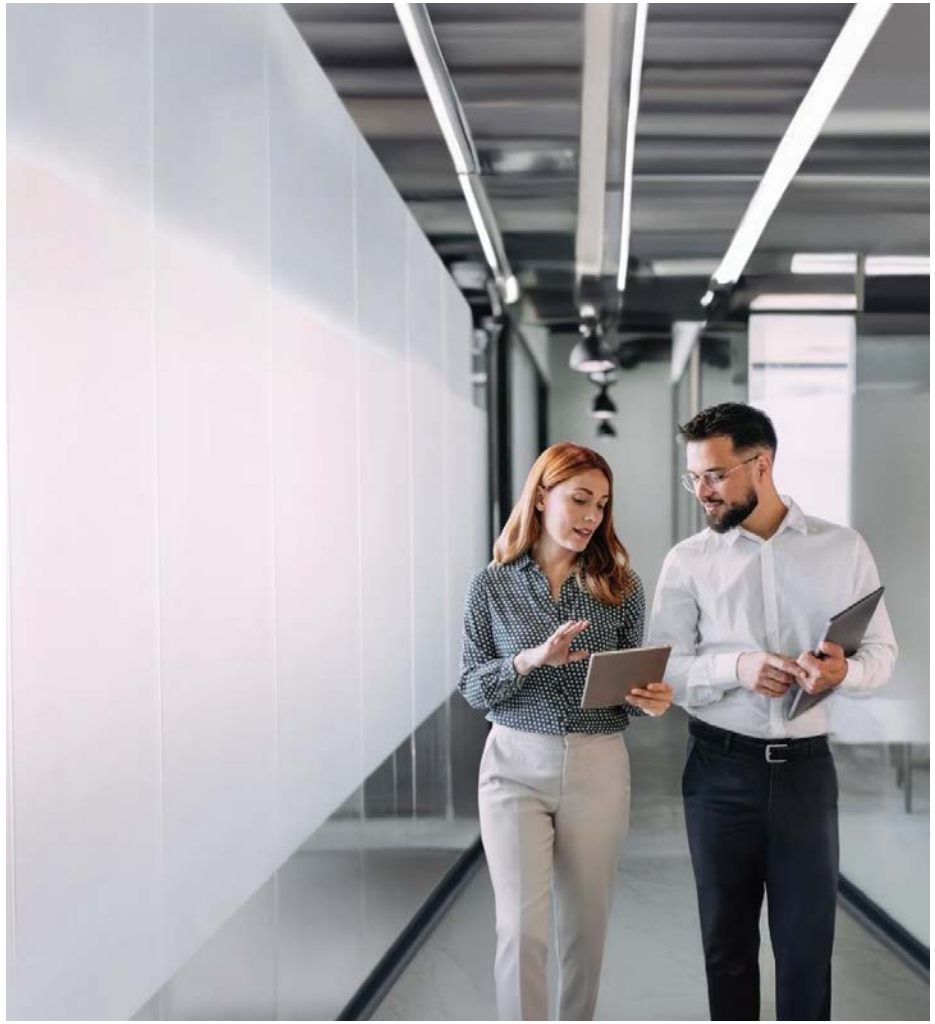
- Assess whether oversight structures, escalation pathways, and reporting channels provide management and the Board with clear, accurate, and timely information on resilience capabilities.
- Review the design and proportionality of reported metrics to confirm they are aligned to the firm's size, business model, and risk profile, and enable stakeholders to make informed resilience decisions.

02
Continuous assurance

- Provide assurance on the effectiveness of remediation activities undertaken by business leads and resilience owners.
- Validate whether vulnerabilities and implemented workarounds have been addressed appropriately, and whether remedial actions have been embedded into future testing cycles to confirm sustained effectiveness.

03
Embedding resilience

- Evaluate how "Day 2" requirements, as outlined by UK regulators, are being operationalized to enhance resilience maturity.
- Review how resilience considerations are embedded into key processes (such as new initiatives, change management, outsourcing, and product approvals) and frameworks (e.g. Third-Party Risk Management (TPRM), Business Continuity, Crisis Management, Cyber Resilience, etc.)
- Assess whether investment in resilience tooling and mapping capabilities is improving speed-to-insight, reducing noise during disruption, and supporting a sustainable long-term resilience strategy.



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 ICT-related disruptions and threats." - Council of EU

DORA is a European regulation that defines detailed and comprehensive requirements for the digital operational resilience of Financial Services firms at an EU level.

Its objectives are to:

- Harmonise local regulations in the financial sector across the EU Member States.
- 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.
- Improve ICT risk management.
- Empower financial supervisory authorities to monitor and audit financial entities and their third-party ICT providers more closely.
- Standardise incident reporting mechanisms and knowledge sharing.

Whilst this is an EU regulation, extraterritorial implications exist:

- Non-EU branches or subsidiaries of EU financial services firms must comply if their ICT operations impact the EU parent or EU-based customers.
- Outsourcing to non-EU providers (e.g. payment processors or cloud vendors) must meet EU supervisory expectations: including full access, audit rights, and compliance assurance.

Key considerations for firms

DORA repositions operational resilience as a strategic priority, with regulatory consequences and clear expectations around ownership, oversight, and demonstrable capability. It requires a mindset shift: resilience is no longer a supporting function; it is a core business responsibility with direct accountability at the regulated entity level.

- Entity-level ownership: In-scope entities must retain direct accountability, even where services are delivered at a group-level or by third-parties.
- Leadership accountability: Senior management must lead resilience efforts and be able to evidence control to regulators.
- Third-party & intragroup oversight: All ICT dependencies must be governed with formal controls (e.g. SLAs, audit rights, exit plans).
- Strategic planning impact: Expansion, outsourcing, and new services must account for resilience capacity and DORA compliance.
- Ongoing obligations: Compliance is continuous, requiring regular testing, reporting, assessments, and improvement cycles.
- Increased regulatory scrutiny: Authorities expect clear, auditable evidence of compliance and readiness.

Ultimately, DORA is not just about preventing outages, it redefines operational resilience as a regulated, measurable, and enforceable capability that must be embedded throughout the business lifecycle.

DORA went live on the 17 January 2025. In-scope firms must be able to effectively transition from a project-style approach of readiness for DORA to operating against the requirements as part of BAU. This can be an area of considerable challenge for firms, and it is necessary to resource appropriately to meet the ongoing expectations now in place.

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

Internal Audit focus areas

01

Validate that remediation actions for gaps identified through the DORA-required ICT risk management framework are timely, effective, and sustainable, with clear evidence of implementation and oversight to strengthen resilience outcomes.

02

Ensure required DORA compliance artefacts and outcomes, such as risk assessments, self-assessments, and digital operational resilience strategies, are complete, accurate, and embedded, providing clear evidence of adherence to regulatory expectations.

03

Assess ICT response and recovery plans as mandated by DORA Article 11, ensuring they are comprehensive, tested, and effective in supporting timely incident response and recovery to maintain operational resilience.

04

Ensure audits of key business processes, even where not DORA-specific, incorporate DORA's prescriptive requirements. For example, reviews of incident management, third party risk, or resilience testing should consider DORA expectations alongside existing objectives.

05

Assess how DORA compliance shifts from project mode to sustainable BAU operations, evaluating readiness, resourcing, and integration challenges that may impact firms' ability to maintain ongoing compliance and resilience.

06

Verify that there is clear ownership and accountability for DORA compliance, ensuring responsibilities are defined and upheld, particularly where regulated entities rely on services delivered within a wider group structure.

07

Ensure the resilience approach is sufficiently robust to deliver resilient outcomes, with scenario testing and related activities that meaningfully challenge critical functions and validate the firm's ability to withstand disruptions.

08

Provide assurance over the ICT risk management framework as required by DORA Article 6, including rules for timely verification and remediation of critical ICT audit findings.

Enterprise Resilience & Crisis Response

Resilience is becoming a critical priority for organisations, including those outside the regulated financial sector, due to rising disruption from cyber threats, climate-related events, supply chain instability, and geopolitical tensions. At the same time, regulatory expectations are increasing with new and emerging frameworks setting clearer standards. These pressures are driving a need for more robust, forward-looking approaches to managing operational risk and maintaining continuity.

Enterprise resilience is now a priority globally across many sectors, driven by a mix of regulatory, geopolitical and market pressures.

In the UK, regulation including the Network and Information Systems (NIS) Regulations, the Telecommunications Security Act (TSA), Critical Third Parties (CTP) regime and Critical Entities Resilience Directive (CERD) are setting clearer expectations for resilience in sectors like energy, telecoms, food, healthcare and digital infrastructure. The focus of Provision 29 of the UK Corporate Governance Code on material risks inherently encompasses those controls linked to resilience, while the UK Government Resilience Framework sets out an approach to build a stronger, more proactive, and integrated resilience system. Meanwhile, the Cyber Security and Resilience Bill, due to become law in 2026, represents a significant modernisation of the UK's cyber security legal framework.

This is taking place while organisations face more frequent and complex disruptions, from cyber threats and climate events to supply chain shocks and political instability. This is raising expectations from boards, regulators and customers for credible, tested plans to maintain continuity during crises.

Internal audit teams will need to adapt their approaches to provide meaningful assurance in this space. Resilience requires forward-looking, dynamic oversight of how important business services (IBS) are protected, how response capabilities are embedded, and how organisations learn and adapt over time.

Key considerations for organisations

Firms should demonstrate they have moved beyond traditional business continuity to embed a holistic resilience programme underpinned by clear governance. This should focus on identifying and mapping IBS that are strategically important to the firm and providing assurance that they can continue to operate within set tolerance thresholds during severe but plausible disruptions. Where tolerances are breached, firms must have effective crisis response structures to manage impacts and restore services quickly and cohesively. Firms should have clearly identified the external experts they have access to, the scope of support from those third parties, and how they are mobilised and managed by the firm during a crisis.

Governance

Ensure governance structures, reporting channels, and metrics support informed decision-making on resilience, aligned to the firm's size and risk profile. Clear ownership and executive sponsorship are essential to provide accountability and drive cultural change.

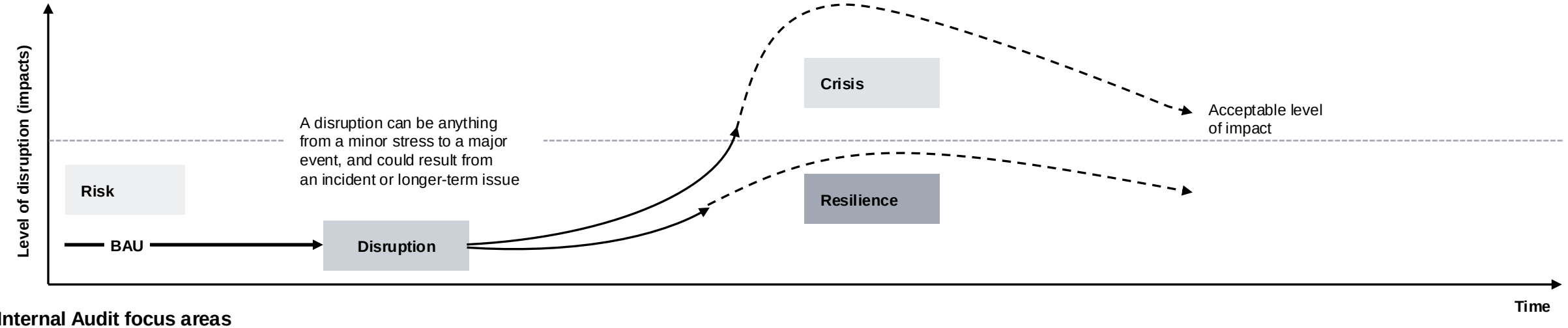
Crisis response

Firms should have clear, tested structures in place to manage crises effectively. This includes crisis plans and scenario-specific playbooks outlining roles, responsibilities, and escalation pathways. External experts should also be identified. Regular testing of these structures helps build confidence, validate effectiveness, and ensure coordinated recovery of key services.

Enabling and embedding resilience

- Demonstrate progress from traditional continuity planning to a mature operational resilience approach: one that enables not just recovery, but also adaptation and evolution through uncertainty. IBS identification and mapping should anchor this effort.
- Embed resilience thinking into new initiatives, change programmes, outsourcing arrangements, and product approval processes. This ensures resilience is considered upfront, not just in response. Support this by investing in technology that improves visibility of critical assets, sharpens situational awareness, and reduces noise during disruption, helping deliver a more agile and sustainable resilience strategy.

Enterprise Resilience & Crisis Response (continued)



Internal Audit focus areas

01
Risk

- Provide assurance that governance structures, reporting channels and reported metrices enable key stakeholders to make informed decisions on the firm's resilience capability, and that they are proportional to the size and risk profile of the firm. A resilience programme should have assigned ownership alongside executive sponsorship to provide accountability and drive cultural change.

02
Resilience

- Assess the extent to which a firm has moved beyond a traditional business continuity focus to a more holistic operational resilience approach. This should enable firms to not only recovery from disruptions but also adapt, evolve and thrive amid ongoing uncertainty. Resilience should be aligned to what matters most to a firm through the identification and mapping of IBS.
- Understand how firms have/can embed resilience considerations into new initiatives, change management, outsourcing, and new product approval processes. Firms can further support their resilience capabilities by investing in the right technology tools to support speed to insight through understanding underlying mapping better, resulting in a reduction of noise in disruption and delivering a sustainable approach to resilience.

03
Crisis response

- Examine the extent to which firms have put in place structures that will enable them to respond effectively to crises. This should include the availability of plans and scenario-specific playbooks that set out team structures, roles and responsibilities, and mobilisation procedures. Firms should have stress tested these structures and rehearsed the capabilities of their response teams (at each level) against plausible, challenging scenarios.

Third Party Risk Management ('TPRM')

The continued increase in the scale and complexity of third-party dependencies, accelerated by rapid digitalisation, is driving a more holistic, proportionate and outcomes-based regulatory focus, with operational resilience at its centre.

Institutions rely extensively on third party service providers, both external and intra-group, for a wide range of services to support their business, including those which are critical to their operations. These dependencies continue to grow in scale and complexity, accelerated by the rapidly increasing use of cloud, AI and other new technologies.

Although continuing to offer firms considerable benefits, including sizeable operational and commercial efficiencies, the risks associated with the use of third parties are pervasive. If not properly managed, they have the potential to significantly impact firms, customers and markets.

Regulation continues to evolve in parallel to these developments, with an extension of the historic focus on outsourcing to a more holistic, outcomes-based focus on broader third-party risk management, with operational resilience at its centre. Key examples here include PRA SS2/21, the EU's Digital Operational Resilience Act (DORA) and the EBA's draft Guidelines on the sound management of third-party risk.

Both DORA and the UK Critical Third Parties regime are also extending supervisory powers to certain third-party service providers with potential implications for financial stability, introducing specific operational risk and resilience requirements.

Despite initiatives towards increased interoperability, regulations continue to vary by jurisdiction. Nevertheless, universally, firms remain fully responsible and accountable for the third-party services they rely on. They are expected to have robust, proportionate processes and controls in place to identify, assess, monitor and manage all risks resulting from arrangements to which they are or might be exposed, aligned to strategy and risk appetite.

Key considerations for firms

Group versus legal entity

Ensuring TPRM frameworks are clear on jurisdictional scope and that key governance processes and controls are set up to support demonstrable senior management control, aligned to Group and regulated entity accountabilities.

Re-wiring TPRM

Greater integration of complementary processes across TPRM, Procurement, Legal and Operational Resilience to promote cross-functional synergies, eliminate gaps or duplication, better manage key dependencies, drive efficiency and enhance resilience.

Integrating new and evolving risk types

Updating TPRM frameworks to integrate processes and controls for identifying, assessing, managing and reporting important new and evolving risk types, including AI and ESG.

Embracing technology

Overhauling legacy systems and technology to support more integrated and proactive risk management, including through leveraging enhanced data models to drive increased risk intelligence and promote more proactive risk monitoring.

Data quality and reporting

Clarity on which data attributes are needed to support which internal and external reporting obligations, and how and where these are collected, with transparency on golden source and ownership, and robust quality controls.

Enhanced assurance and oversight

Ensuring contractual terms support access, audit, and information requirements, leveraging emerging third-party service provider reporting where possible, while ensuring that the use of any pooled audits or third-party certifications is appropriate to the scope of services received.

Third Party Risk Management ('TPRM') (continued)

Internal Audit focus areas

01

Third-Party risk management framework

Confirm that the firm's framework for managing third-party arrangements, including the TPRM policy(/ies), complies with applicable laws and regulations, is effectively implemented, and aligns with Board approved strategy and risk appetite.

02

Risk assessments and due diligence

Assess the adequacy, quality, and effectiveness of criticality/materiality assessments and broader third-party risk assessments, including initial and ongoing due diligence.

03

Governance and oversight

Evaluate the involvement and oversight of relevant governance bodies in the approval, monitoring, and management of third-party arrangements.

04

Monitoring and ongoing management

Review the monitoring mechanisms and management practices in place for third-party arrangements to ensure they remain effective and proportionate.

IA reviews for this area should align with reviews of operational resilience and applicable risk areas, assessing the design and operating effectiveness of processes and controls to enable the firm to protect itself from threats and potential disruption, including response and recovery capabilities. Follow-up processes for findings should also be formalised, including the timely verification and remediation of material audit findings.

Data – Evolving Regulation

The regulatory landscape for data is continually evolving, spanning data protection and privacy, AI governance, digital operational resilience, and industry-specific reporting standards.

The regulatory landscape for data is continuing to evolve across the UK and EU, reshaping how organisations govern, protect and use information. The UK Data Use and Access Act (DUAA) represents the most significant reform to UK data protection law since GDPR. It introduces new flexibilities for data reuse, automated decision making and smart data access, while also simplifying the rules for international transfers and enhancing enforcement powers.

At the same time, the EU Artificial Intelligence Act establishes strict obligations for high-risk AI systems. These include expectations around data quality, transparency and documentation, which are particularly relevant for UK-based businesses operating in the EU. Alongside this, the EU Digital Operational Resilience Act brings data integrity, availability and traceability to the forefront of ICT risk management for financial services.

Internal audit teams must assess whether their organisations are staying ahead of these regulatory changes: not just in policy, but in operational practice. Increasingly, compliance requires more than written controls; it demands robust data governance, accurate records, and end-to-end traceability of data usage across business lines and platforms.

Key considerations for firms

Understand and scope the evolving obligations

Regulatory changes vary by jurisdiction, industry, and domain. Organisations should identify regulatory changes (e.g. DUAA, EU AI Act, DORA, etc.) impacting their organisation and understand how the rules impact them.

Integrate regulation into data and AI governance

Firms should ensure their AI and data governance structures can evidence compliance with regulatory expectations, including model transparency, lawful basis for processing, data minimisation, and data subject rights management. This includes clear ownership, audit trails, and integration with policy frameworks.

Operationalise new requirements, not just document them

Organisations must embed regulatory changes into operational processes, not just update policies. For example, under DUAA, Data Subject Access Request (DSAR) handling procedures must reflect the new rules on response timelines and “reasonable and proportionate” search standards.

Reassess GDPR remediation with a fresh lens

As enforcement sharpens, organisations should revisit previous IA actions relating to GDPR. This includes verifying that mitigations are sustained, records are current, and that risk registers reflect known vulnerabilities.

Data – Evolving Regulation (continued)

Internal Audit focus areas

01

Assess regulatory readiness

Review whether the organisation maintains an accurate, centralised register of applicable data and AI-related regulations.

02

Evaluate DUAA implementation readiness

Assess whether the organisation has completed an impact assessment comparing the existing privacy framework to the DUAA requirements and evaluate whether the conclusions drawn have been appropriately addressed through changes to policy and processes.

03

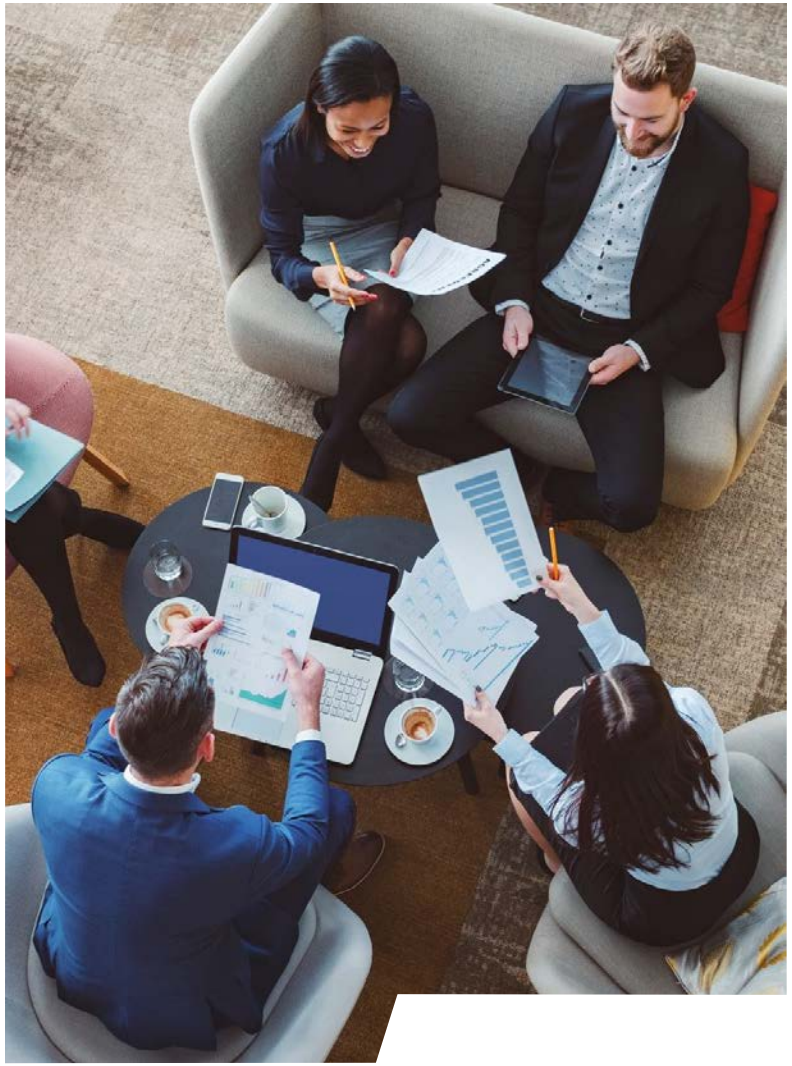
Review AI governance for regulatory alignment

For high-risk AI use cases, assess whether data quality controls, bias detection mechanisms, and model documentation comply with AI Act requirements. Confirm that lineage, testing protocols, and human-in-the-loop safeguards are demonstrable and actively monitored.

04

Test sustainability of prior GDPR controls

Reassess previous findings and confirm whether remediation remains effective.



Data – Strategy Reset

Organisations are reassessing their enterprise data strategies to stay competitive in a landscape dominated by AI and advanced analytics.

A robust data strategy sets the blueprint for how an organisation collects, governs, manages and leverages data to drive its strategic objectives. Far beyond a technology or compliance document, a data strategy enables businesses to unlock tangible value, from alignment in investment to risk reduction. In today's landscape of proliferating data, increasing regulatory scrutiny, and rising AI adoption, the absence of a coherent, adaptive data strategy often results in siloed ownership, inconsistent standards, and suboptimal outcomes.

At its core, a data strategy typically defines the organisation's data vision, governance structure, key use cases, and roadmap for capabilities across architecture, platforms, people, and processes. It sets out how data supports enterprise priorities.

Static strategies quickly fall behind. The market is evolving at pace, driven by generative AI, cloud-native architectures, digital operational resilience regulation, and shifts in customer and shareholder expectations. Data strategies that were relevant even 18 months ago may now lag behind regulatory, architectural or business model changes. Organisations must treat their data strategy as a living document, revisited and refined regularly to reflect emerging technologies, new value drivers, and shifting risk landscapes.

Key considerations for firms

Strategic alignment and value prioritisation

Data strategies should be explicitly linked to the organisation's business objectives and plans, whether focused on growth, transformation, or risk mitigation. Initiatives should be sequenced based on value, with defined Key performance indicators (KPIs) that tie directly to measurable commercial, operational or risk outcomes.

Embedding data literacy and cultural change

Technical success is insufficient without human adoption. Organisations must embed data literacy at all levels: from executive understanding of AI and data ethics to frontline use of dashboards and insights. Leadership sponsorship, incentivisation and education are key levers.

Balancing central and federated delivery models

Many organisations are now combining data fabric technologies, with their focus on unified access, metadata, and governance with data mesh principles that place accountability for data with business domains. A strong data strategy should clearly define which elements remain centrally governed (e.g. data policies, architecture standards, compliance, etc.) and where domain teams are empowered to own and manage data as products.

Performance management and accountability

Firms should establish clear governance structures (e.g. data councils, stewardship forums) and track progress using enterprise-wide metrics such as data issue closure rates, data usage trends, or business case delivery. Strategy reviews should be built into planning cycles.

Data – Strategy Reset (continued)

Internal Audit focus areas

01

Strategic alignment and oversight

- Evaluate the adequacy of data strategy, ensure that it is formally approved and regularly reviewed at executive level, with clear links to business objectives and value delivery.

02

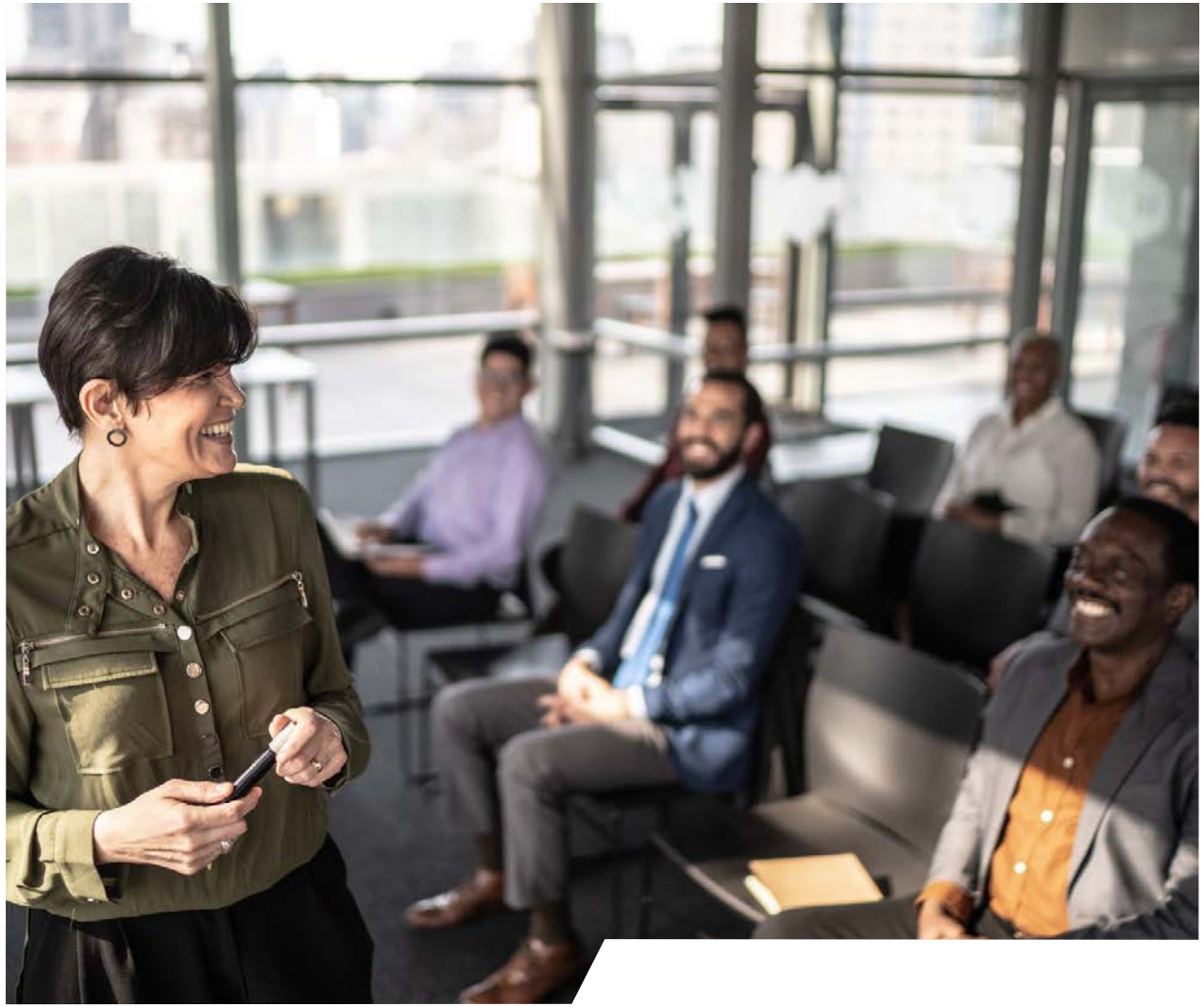
Governance and accountability

- Assess whether roles, controls and ownership structures are clearly defined and operating effectively.

03

Culture and change management

- Evaluate how well data literacy, performance metrics, and change initiatives are embedded across the organisation to support sustained adoption and impact.
- IA should also review whether cultural factors and change management practices are enabling the adoption of new ways of working and supporting sustainable transformation.



Data – AI-Ready Foundations

With the explosion of generative AI and advanced analytics, the quality and governance of data feeding these models has become critical.

Organisations across sectors are investing in AI to streamline decisions, personalise customer experiences, and unlock operational efficiencies. AI's impact potential is vast – but its success is fundamentally dependent on the adequacy of the data it consumes. Models are only as effective and fair as the data that feeds them. As regulators and boards increase scrutiny over explainability and outcomes, the need for robust data foundations has never been more pressing.

Many firms have been overestimating their AI readiness. Initial proof-of-concepts or attempts to scale solutions have often exposed weaknesses: fragmented data, inconsistent standards, and legacy infrastructure. These gaps reflect overconfidence in perceived data maturity, a lack of formal data governance, and insufficient investment in the roles and platforms needed to sustain enterprise-scale AI.

Organisations must strengthen core data management capabilities. That includes improving data quality and completeness, embedding clear metadata standards to support transparency and discovery, and maintaining lineage from raw inputs through to model outputs. Data must be continuously monitored, supported by governance frameworks that define ownership, oversight, and issue management processes. Without this foundation, AI solutions may not be trusted.

Key considerations for firms

Assess and remediate foundational data capabilities

Organisations should conduct data management maturity assessments, examining whether standards and practices are fit-for-purpose. These assessments often reveal "unknown unknowns", such as applications failing to meet standards and poor transparency of data flows (e.g. undocumented transformations and calculation logic). Addressing these issues early, in line with the capabilities you need set-out by your data strategy, reduces rework and builds trust in AI outcomes.

Reinforce traceability, explainability and trust

As regulatory scrutiny increases, organisations must demonstrate how AI models reach decisions and how underlying data is governed. This requires enterprise-wide standards for lineage, metadata, and versioning, plus well-defined ownership and oversight. Without this, organisations risk reputational damage, regulatory non-compliance, and poor customer outcomes.

Ensure readiness before scaling AI use cases

Before scaling AI solutions, organisations must ensure they have strong data foundations in place. This means verifying that data pipelines are stable, well-governed, and continuously monitored with clear accountability for detecting and resolving quality or integrity issues.

Embedding controls "by design" from the outset enables sustainable AI adoption: this ensures that AI initiatives deliver measurable value aligned to business objectives, while keeping associated risks within acceptable boundaries

Data – AI-Ready Foundations (continued)

Internal Audit focus areas

01

Test data management maturity

Review whether management's self-assessment of AI readiness is supported by evidence, e.g. data lineage maps, data quality metrics, data catalogue usage, etc. Alternatively, evaluate the organisation's data management policy framework and current-state data landscape against industry benchmarks (e.g. DAMA-DMBOK*), and assess whether the capabilities in place are sufficient to support the prioritised use cases outlined in the data strategy.

02

Evaluate controls across AI-data pipelines

Assess whether data sourcing, transformation and integration processes supporting reporting and AI are documented, tested, and governed. Verify if continuous monitoring for data drift, missing values or outliers is in place and leads to actionable remediation.

03

Review governance forums and issue escalation

Confirm that data and AI governance structures are active, cross-functional, and empowered to challenge data use in reports and AI models. Audit trails should demonstrate accountability for approvals, exceptions, and issue resolution.

*DMA-DMBOK - the Data Management Association's Data Management Body of Knowledge7.5

Data – 'Dark' Data and Unstructured Information

Organisations typically amass extensive information assets that remain poorly managed and under-utilised.

Unstructured data such as emails, chat logs and collaboration platform content continues to accumulate rapidly across most organisations. Much of it is unclassified, unmonitored and non-compliant with enterprise policies. This "dark data" often exists outside systems of record. As a result, many organisations face mounting challenges around discoverability, over-retention, and inconsistent archival and deletion practices.

These ungoverned assets increase exposure to data breaches, regulatory non-compliance and costly eDiscovery or legal hold processes. In the context of tightening privacy regulation, organisations must be able to demonstrate effective controls over where personal and sensitive data resides, including outside core systems.

Leading organisations are shifting to a proactive, risk-based approach to managing dark data. This includes defining targeted remediation objectives, such as identifying and securely deleting redundant, obsolete or sensitive data and deploying automated discovery tools to improve visibility. Accountability is embedded through appointed Data Owners and Data Stewards who coordinate structured reviews and champion enforcement of policy-aligned retention and disposal practices.

Key considerations for firms

Understand the profile and scale of dark data

Organisations should conduct structured discovery and risk assessment exercises to establish where unstructured data resides, whether sensitive or regulated data is present, and how current practices compare to internal standards on retention, archival and deletion. Discovery tooling and sample audits can help identify key policy gaps and high-risk repositories (e.g. shared drives, personal inboxes, legacy archives).

Automate and embed lifecycle controls

Leading firms are deploying automated tools to enforce retention and disposal policies for unstructured content across collaboration platforms, cloud storage and on-premises systems. Policy configuration should reflect legal, regulatory and business needs, with capabilities for exception handling and audit logging.

Adopt a risk-based approach to remediation

Not all dark data presents equal risk. Firms should define prioritised objectives, such as removing unneeded personal data, isolating records subject to litigation hold, or cleaning up legacy project files, and target interventions where the potential for regulatory exposure, cost or operational inefficiency is greatest.

Strengthen governance and ownership

Clear accountability is essential. Appointing Data Owners and Data Stewards for business domains ensures local oversight, while enterprise policies set consistent standards. Governance forums should review progress against dark data reduction targets and report on policy compliance, breach risks and remediation outcomes.

Data – ‘Dark’ Data and Unstructured Information (continued)

Internal Audit focus areas

01

Evaluate unstructured data governance

Review whether the organisation’s data policies cover unstructured data and that roles, responsibilities and interactions are clearly defined for policy enforcement, remediation and ongoing monitoring.

02

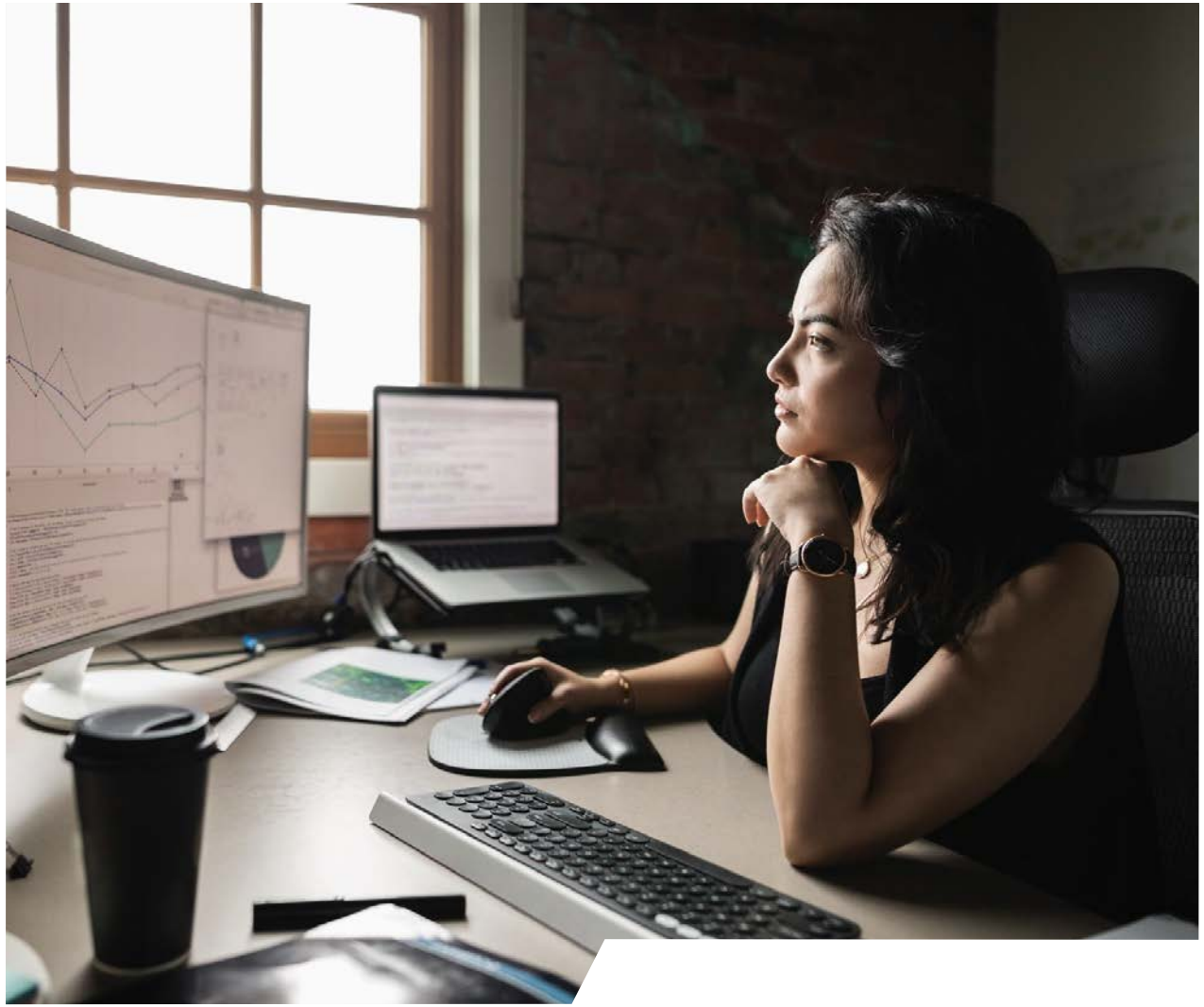
Test discovery and classification capabilities

Assess whether the organisation has conducted recent scans or classification exercises on unstructured data stores (e.g. file shares, SharePoint, email, etc.) to identify sensitive or high-risk content, and whether discovery tools or manual reviews are consistently applied across business areas.

03

Review retention and disposal enforcement

Validate whether manual or automated controls are in place to apply retention schedules, execute secure deletions, and evidence ongoing compliance. Consider testing specific repositories for unused content or records beyond documented retention limits.



Data – Data Risk

Organisations are increasingly recognising data as a standalone enterprise risk category, with linkages to privacy, operational resilience, and AI governance.

Enterprise Risk Management (ERM) frameworks provide organisations with a structured approach to identifying, assessing and managing the range of risks that could impact their ability to meet strategic objectives. These frameworks typically group risk into categories, such as operational, compliance and financial, and define processes for risk ownership, escalation, appetite-setting and control monitoring.

Data risk refers to the potential for adverse outcomes arising from poor-quality, unavailable, misused, or uncontrolled data. As data becomes more tightly linked to customer trust, AI oversight and external reporting, firms face heightened scrutiny from boards, regulators and the public on how data is used, protected and governed.

In response, organisations are now seeking to gain greater clarity over data risk. This includes deciding where and how data risk should be captured within the ERM and developing key risk indicators to measure exposure. Some firms have chosen to embed data risks across existing risks (e.g. embedding data quality metrics into operational risk), while others are establishing a standalone data risk with a dedicated owner and board-level reporting. Choosing the right model depends on the firm's maturity, risk profile and cultural appetite for cross-functional governance.

Key considerations for firms

Define what data risk means for your organisation

Data risk is multi-dimensional; spanning quality, availability, integrity, misuse, privacy, and security. Organisations should ensure their definition of data risk is tailored to their risk taxonomy and unique operational characteristics, and that it is clearly understood by risk owners across the business.

Develop meaningful metrics and escalation criteria

Identify and monitor leading indicators of data risk, such as material data quality issues in critical reports, control failures in AI models, or high volumes of data privacy incidents. Ensure these metrics feed into ERM dashboards, influence risk appetite discussions and trigger appropriate remediation where tolerances are breached.

Assess how data risk is captured in the ERM framework

Decide whether data risk should be embedded across existing risk types (e.g. operational, compliance, model risk, etc.) or captured through a dedicated data risk stripe. This should reflect the organisation's risk profile, regulatory exposure and maturity in data governance. Whichever model is chosen, ownership, escalation routes and KRI definitions must be clear and enforceable.

Establish governance and reporting mechanisms

Data risk should be routinely discussed at senior governance forums and linked to strategic and operational priorities. This includes ensuring adequate reporting to risk committees, ownership by accountable executives, and integration with broader initiatives like AI oversight and resilience.

Data – Data Risk (Continued)

Internal Audit focus areas

01

Review how data risk is defined and captured in the ERM framework

Assess whether the organisation has clearly articulated its data risk profile, and whether data risks are appropriately embedded across existing stripes or managed through a standalone risk category with defined ownership and board visibility.

02

Evaluate the design and use of data risk metrics and reporting

Test whether key risk indicators (e.g. data quality exceptions, reporting errors, privacy incidents, etc.) are tracked, linked to appetite, and trigger escalation. Confirm whether governance forums receive timely, insightful reporting to support effective oversight and remediation.

Sustainability - Preparing for UK SRS

On 25 June 2025, the UK Government released a package of three consultations[1] representing the first phase of work to modernise the UK's sustainability reporting and assurance framework. This included a consultation on the new UK Sustainability Reporting Standards (UK SRS) exposure drafts.

The consultation is the culmination of the UK's work on assessing the suitability of the International Sustainability Standards Board (ISSB) Standards on the general requirements for the disclosure of sustainability matters International Financial Reporting Standards (IFRS) (IFRS S1) and climate-related disclosures (IFRS S2) for the UK market.

Whilst there is broad alignment to the global ISSB standards, there are minor amendments currently proposed:

1. References to Sustainability Accounting Standards Board (SASB) amended to 'may refer', making use of these sectoral standards optional.
2. Extend 'climate-first' transition relief for IFRS S1 by one year, allowing entities to focus solely on climate-related disclosures for the first two years.
3. Requirement to use Global Industry Classification Standard (GICS) for disclosing financed emissions removed, allowing the use of other classifications.

Key considerations for firms

Monitoring global developments

UK SRS will only apply to UK entities, but over 30 countries are currently in the process of adopting the related ISSB standards, with over 10 already initiating their national adoption proceedings. As each country has the option to amend the requirements, it is important to track these updates globally and consider the implications of the jurisdictional nuances, including on global reporting consistency and resource constraints.

Leveraging existing work

There is significant interoperability between ISSB and key sustainability standards such as the Corporate Sustainability Reporting Directive (CSRD), European Sustainability Reporting Standards (ESRS) and Taskforce on Climate-related Financial Disclosures (TCFD). Therefore, firms already reporting under these requirements can leverage and tailor their previous efforts, such as in performing a materiality assessment, to support their response to UK SRS requirements.

Begin 'No Regret' actions

Whilst the exact timing for UK SRS application is still to be confirmed, there are a number of actions firms can take to prepare for ISSB with confidence and support a successful implementation. For example:

- Reviewing existing materiality assessments, such as a CSRD-aligned double materiality assessments or financial risk assessments, to identify enhancements required for UK SRS compliance.
- Performing a readiness assessment comparing existing sustainability disclosures to ISSB requirements, identifying gaps and associated mitigation actions.
- Additionally, although assurance is not yet mandatory for UK SRS, the consultation signals that it may be expected in the future. It may be helpful for firms to review the extent to which their current reporting processes and policies comply with existing assurance standards.

Keeping track of updates

- The consultation is open until 17 September 2025. Following this, further consultations will address how the UK SRS are integrated into the UK reporting framework and which entities fall in-scope. Firms should monitor these consultations to be enable a quick response to any future amendments and to identify future in-scope entities in a timely manner.

[1]Consultations include: UK Sustainability Reporting Standards, Developing an oversight regime for assurance over sustainability-related financial disclosures, and Transition plan requirements.

Sustainability - Preparing for UK SRS (continued)

Internal Audit focus areas

01

Review and assess the effectiveness of the implementation programme developed to comply with the UK SRS requirements, once rules are finalised. Focus should be on ensuring firms align with the regulators' expectations and any jurisdictional nuances that deviate from global standards.

02

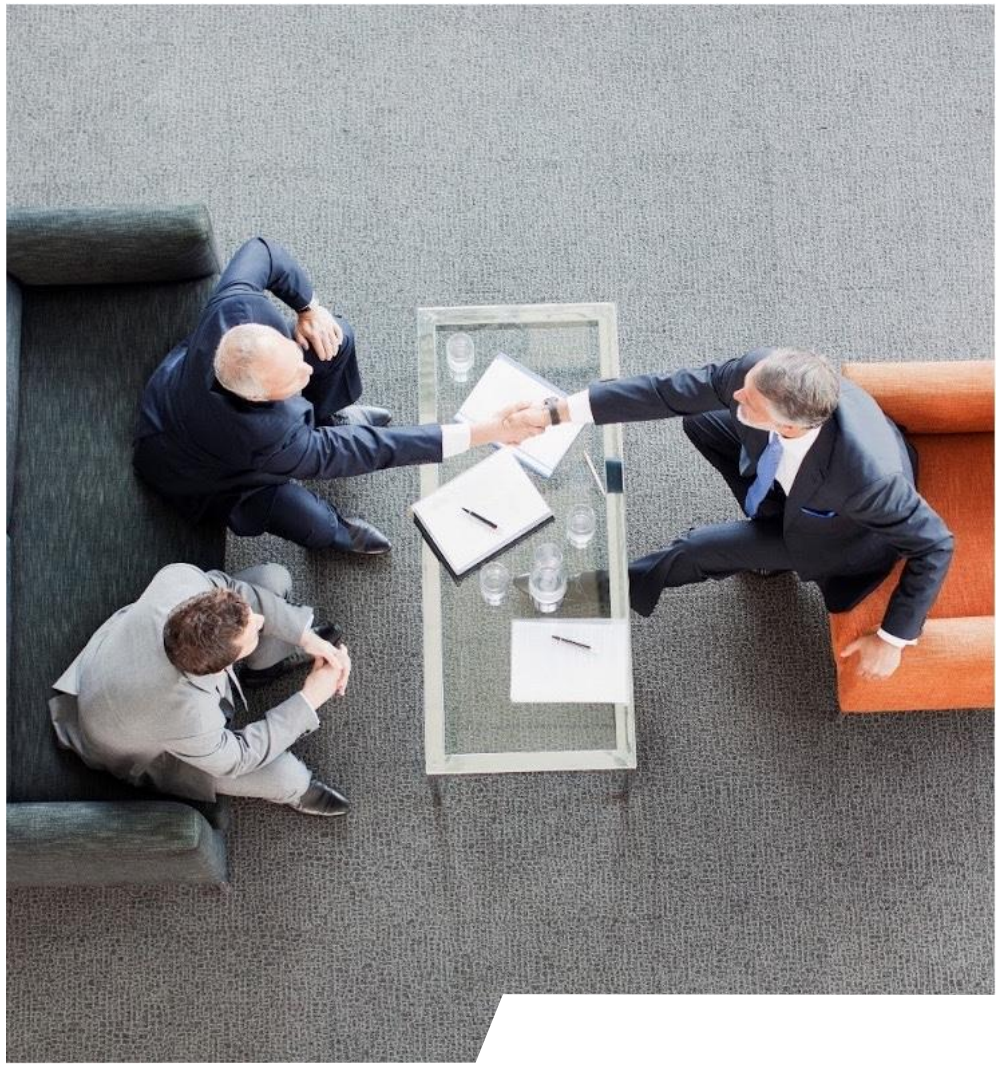
Review of materiality assessment process, including the determined thresholds for materiality. The review should include assessing any difference in outcomes between UK SRS materiality assessments and other sustainability materiality assessments, such as under CSRD, if it has been performed.

03

Review governance procedures, including sign off and decision-making process, for new methodologies, regulatory interpretations and external disclosures.

04

Assess the quality of technology and data systems, policies and controls that may be required for UK SRS reporting to identify required enhancements ahead of external reporting. Enhancements may include increasingly granularity of data to be available at subsidiary level, tightening and documenting controls over data manipulations and reviewing access protocols for sensitive information.



Sustainability - Transitioning to Net Zero

With legally binding UK Net Zero targets and regulatory momentum building, firms must shift from ambition to action when developing their transition plans to protect their businesses from the risks of a hot house or disorderly transition scenario and, if desired, contributing to a Net Zero economy.

In its manifesto, the Labour government committed to requiring UK-regulated financial institutions and certain other large companies to develop and implement credible transition plans that align with the 1.5°C goal of the Paris Agreement.

To deliver on this, the UK Government is consulting on four key aspects of transition plans:

- Whether transition plans should be mandatory, or if a 'comply or explain' approach should be introduced as a transitional step
- Expanding the scope to include economically significant firms in the UK
- Exploration of whether there should be a legal requirement to deliver on transition plans
- Whether and how transition plans should align with national and international climate and environmental goals

Various frameworks are being suggested that companies may have to comply with, including the Transition Plan Taskforce (TPT) framework and UK SRS.

Key considerations for firms

Track regulatory developments:

Firms should closely monitor UK and international regulatory developments to stay prepared for evolving transition planning expectations and ensure strategic alignment across global regimes.

Challenges for firms with global presence:

Firms operating across multiple jurisdictions may face challenges in meeting diverse regulatory requirements. It is crucial to track and manage these jurisdictional nuances to ensure compliance and consistency in global reporting.

Evaluate alignment with emerging standards:

This should include UK SRS S2 and frameworks like TPT, to ensure regulatory compliance and strategic coherence.

Conduct a readiness assessment:

Identify existing elements of transition plans and determine whether foundational work or enhancements are needed. Elements of Transition Planning material will exist in other sustainability initiatives previously undertaken.

Consider broader drivers and opportunities:

Such as commercial trends and value creation potential, when refining or developing transition planning approaches.

Align transition plans with corporate strategy:

Ensure transition plans are actionable and embedded into business decision-making, supported by robust governance, clear timelines, and adequate resources. Transition plans should be aligned with the firm's overall business and corporate strategy to ensure coherence and effectiveness in achieving sustainability goals

Sustainability - Transitioning to Net Zero (continued)

Internal Audit focus areas

01

Validate any targets set, assessing actions planned to meet the targets to ensure they are actionable and effective. This should also involve a review of timelines set to assess whether they are realistic.

02

Review quality of data being used to set targets and develop actionable plans, flagging areas that require increased granularity in order to effectively track progress.

03

Assess governance pathways, ensuring that the Board is appropriately involved in developing the plan and remains informed of the progress against it. This will include ensuring that transition planning initiatives are aligned to the corporate strategy and planning process

04

Review policies underpinning the transition plan, ensuring they are documented and support its implementation.

Sustainability - Embedding Sustainability into BAU processes

Firms are increasingly viewing ESG considerations strategically and embedding them into existing operating models in order to capitalise on opportunities. This also reflects the growing expectations to integrate climate, nature and social factors into risk management processes.

As firms seek new sources of value, many are embedding sustainability into strategy and day-to-day operations to strengthen risk management, unlock revenue growth, and build long-term resilience. Integrating sustainability across core business pillars and operating models can streamline processes, deliver cost efficiencies, and prepare organisations for evolving reporting requirements.

This shift aligns with rising regulatory expectations for sustainability to be embedded within risk management, as reflected in the PRA's climate risk consultation for banks and insurers (CP10/25).

Firms should ensure sustainability-related risks and transition planning assumptions are incorporated into corporate plans, capital and liquidity adequacy assessments, stress testing, and scenario analysis. Governance and oversight structures must also support the effective integration of these risks into forward-looking planning.

Key considerations for firms

Governance and oversight

Successful integration requires adequate senior management accountability and awareness. The Board and other appropriate senior management forums must remain informed of the impact sustainability matters have on the business and should be actively involved in overseeing any associated risks. This involvement should be throughout the end-to-end process, including through supporting the setting of thresholds to determine material matters and monitoring mitigation factors for sustainability risks. Maintaining this awareness will require good quality MI.

Data quality

Sustainability information is increasingly being reported alongside financials. As a result, there is a growing need for a swift improvement on the quality of this data in order to match the standards expected of financial information. Continuing to utilise poor quality sustainability data can lead to incorrect assumptions being embedded into business and financial analysis, leading to poor strategic decision making and increasing regulatory and reputational risk.

Stakeholder engagement

Successfully embedding these considerations requires buy-in from a number of functions to ensure it is being applied consistently. This will likely require upskilling for functions and stakeholders who have historically been on the periphery of sustainability.

Assess strategic priorities

Before enhancing operating models, firms must have a thorough understanding of their strategic sustainability priorities, including the issues most material to them and their intersection with the wider business. This helps the stakeholder engagement process and provides a central purpose the firm can rally behind.

Technology

Successful integration relies on adequate data and tools to capitalise on opportunities and ensure efficiencies. Where tools exist to support this, they should be reviewed to assess their adequacy and to improve the control environment. This can include an assessment of processes and policies. Where data and technology capabilities are more immature, cost-benefit analysis can be performed to understand the implications of implementing various third-party tools in comparison to building an in-house solution.

Sustainability - Embedding Sustainability into BAU processes (continued)

Internal Audit focus areas

01

Assess how sustainability considerations have been embedded into existing mechanisms. For example, a review of the investment process should focus on any new steps included to assess the prospective investment's compatibility with the firm's sustainable investment goals, such as alignment with the firms' supplier emission targets or compliance with minimum human rights standards.

02

Review ESG data practices against firm data governance and quality standards, identifying areas for improvement. Focus should be on ensuring that the data is of sufficient quality and granularity to accurately and effectively be utilised in metric calculations and forecasting, where relevant.

03

Assess integration of sustainability considerations into risk management processes, which could include an independent review of climate risk frameworks and an assessment of whether and how climate risk factors have been embedded into operational risk controls, product approvals and credit policies, where relevant.

04

Review processes to ensure senior management oversight. This may include assessing whether there is a clear governance structure with accountability mapping across Board, executive and risk functions, whether senior management receives periodic training on sustainability matters, and the frequency at which the Board reviews climate risk considerations.

05

Review supply chain processes with a particular view on Sustainability. In particular, reviewing procurement procedures for due diligence, on-boarding and on-going monitoring in relation to environmental topics such as emissions and nature, as well as social topics such as modern slavery. Many firms will already have mature processes for the latter, however third-party risk management as it relates to environmental topics is nascent.

Diversity, Equity and Inclusion (DE&I)

Global DE&I strategies are facing growing legal, regulatory, and reputational scrutiny. While expectations for fairness, equity, and inclusion continue to rise worldwide, the landscape is shifting unevenly. In the US, a wave of litigation, legislative rollbacks, and political opposition is challenging longstanding DE&I efforts. In contrast, the UK and EU are maintaining, if not intensifying, their focus on inclusive practices, backed by evolving regulatory frameworks. There is need for strong oversight to ensure that organisations stay ahead of global developments and ensure their DE&I policies are intentional, well-designed, and demonstrably effective.

Three key DE&I developments shaping the risk agenda for 2026

01 Global DE&I Backlash: Legal and Reputational Risk in the US

In the United States, DE&I initiatives are facing growing political and legal challenges. Following the 2023 Supreme Court ruling on affirmative action and the 2024 Presidential Election, corporate diversity programmes are now subject to heightened legal and reputational risk.

This includes lawsuits challenging race-conscious hiring practices, board diversity requirements, and supplier diversity efforts. Although these developments are primarily US-focused, they carry cross-border implications for global employers whose DE&I strategies are not confined to one jurisdiction.

02 Pay Transparency and Equity

Across Europe and the UK, legislative pressure is mounting to close pay gaps and increase employer transparency. The EU Pay Transparency Directive, which came into force in 2023 and aims to ensure equal pay for equal work between men and women, requires all member states to implement legislation by 7 June 2026. The Directive includes several pay transparency measures, including requiring employers to:

- Disclose pay ranges within the recruitment process;
- Share average pay for men and women in comparable roles with employees upon request;
- Provide workers with access to the criteria to determine pay, pay levels and pay progression;
- Regularly disclose gender pay gaps and pay gaps by category of worker; and
- Conduct joint pay assessments when gaps exceed defined thresholds and are not supported by gender-neutral factors.

With transparency obligations under the EU Pay Transparency Directive taking effect from 7 June 2026, and reporting due by June 2027 on 2026 data, organisations cannot afford to delay preparation. Many are already aligning job architecture to the Directive's requirements and conducting privileged equal pay analyses to identify and address potential gaps ahead of enforcement.

In the UK, momentum is also building through the draft Equality (Race and Disability) Bill, which proposes extending pay gap reporting to ethnicity and disability. Following the 2025 government consultation, the expected framework mirrors existing gender pay gap rules, with an emphasis on consistency, comparability and accountability. Although the bill is still progressing through legislative channels, the policy intent is clear. As a result, organisations are increasingly prioritising diversity data collection and voluntarily calculating ethnicity and disability pay gaps to prepare for the additional reporting obligations.

Diversity, Equity and Inclusion (DE&I) (continued)

03 Inclusion and Workplace Rights: The Employment Rights Bill

The UK Government's Employment Rights Bill, part of the 'Make Work Pay' reforms, sets out wide-ranging workplace changes, with most measures due in 2026 and 2027. These include day one unfair dismissal protection from 2027 and earlier reforms to industrial relations, such as ballot rules and strike protections, expected to take effect upon Royal Assent in late 2025.

Whilst there are many changes due to take place over 2026 and 2027, those that currently appear to be most pertinent to internal audit are as follows:

Change	Date change is due
Provision of day one rights for paternity leave and unpaid parental leave,	From April 2026
Requirement for employers to take **all** reasonable steps (instead of 'reasonable steps') to prevent sexual harassment.	October 2026
Employer liability if employees are harassed by third parties.	October 2026
Gender pay gap and menopause action plans which require employers to outline how they are address gender pay gaps and support employees through menopause.	From 2027 but can report from a voluntary basis April 2026

Key considerations for firms

Align policies with jurisdictional requirements

Ensure DE&I strategies reflect the legal and cultural landscape of each operating region, particularly where US legal pushback may conflict with EU and UK inclusion mandates.

Strengthen data infrastructure

Build robust systems to collect, validate, and report diversity and pay data, including gender, ethnicity and disability metrics, to meet anticipated regulatory standards.

Prepare for pay transparency obligations

Review and update job architecture, grading structures and pay criteria to comply with the EU Pay Transparency Directive and support equal pay readiness.

Adapt policies to reflect upcoming UK employment reforms

Assess the impact of new UK statutory rights and regulatory enforcement mechanisms and update internal policies and processes accordingly.

Deliver credible and measurable DE&I action plans

Meet stakeholder expectations by ensuring DE&I initiatives are supported by clear KPIs, tracked outcomes and transparent reporting on hiring, progression and retention.

Diversity, Equity and Inclusion (continued)

Internal Audit focus areas

01

Review policies and governance frameworks

Review DE&I policies, governance frameworks, and relevant training materials to ensure alignment with jurisdiction-specific legal standards, especially where US litigation risk may conflict with global DE&I commitments.

02

Assess data collection and reporting readiness

Evaluate whether there is robust and effective framework to ensure that demographic and pay data is collected lawfully, consistently, and accurately, with systems capable of calculating and reporting pay differentials by gender, ethnicity, and disability.

03

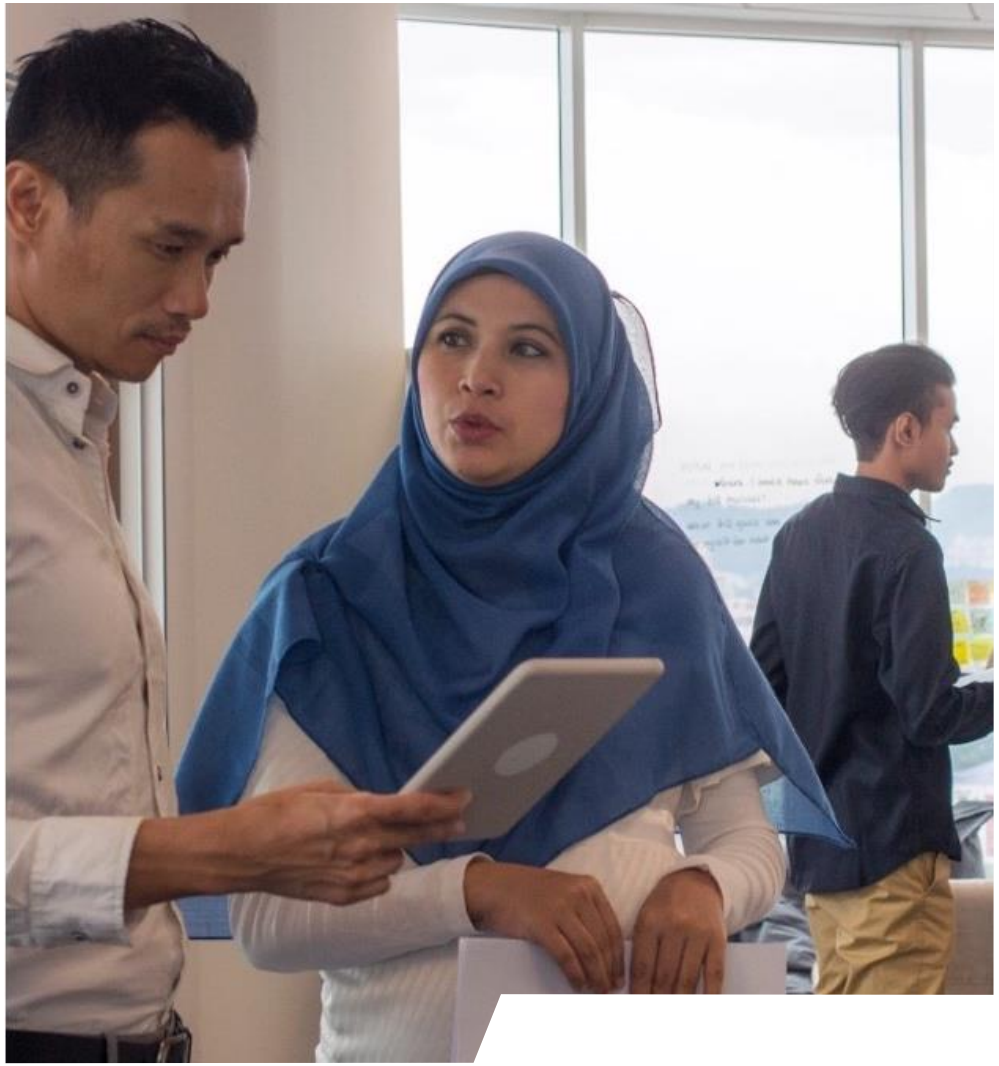
Assess compliance preparedness for EU and UK reforms

Determine whether the organisation has identified in-scope EU operations and is prepared to meet pay transparency requirements, including pay band reporting, promotion tracking, and defensible grading structures. Review alignment with UK Employment Rights Bill reforms such as leave entitlements and anti-harassment obligations.

04

Audit the quality and impact of action plans

Examine whether gender and broader DE&I action plans developed by the organisation are measurable, monitored through clear KPIs, and linked to tangible outcomes such as hiring, progression, and retention.



Non-financial misconduct

The FCA has confirmed that non-financial misconduct will be formally incorporated into the Conduct Rules. Firms are expected to assess, manage, and remediate behavioural risks with the same rigour as other forms of misconduct.

The FCA published a policy statement and consultation paper CP25/18 on 2 July 2025, confirming a final rule to embed non-financial misconduct (NFM) in its Code of Conduct (COCON). The new COCON rule makes it clear that for all SM&CR firms (FSMA firms with a Part4A permission), whether banks or non-banks, the scope of the Conduct Rules covers serious instances of bullying, harassment and similar behaviour in the workplace.

The FCA is also re-consulting on detailed guidance on this rule, as well as guidance which would explicitly confirm that bullying, harassment and similar misconduct (both in the workplace and personal life) are relevant to 'fit and proper' requirements.

The paper follows CP23/20, which proposed NFM changes as well as wider diversity and inclusion (D&I) proposals in September 2023. The wider D&I proposals are no longer being taken forward, as confirmed by the FCA in March 2025. The FCA also shared findings of a survey last year of how wholesale firms detect and handle incidents of NFM.

The new COCON rule will come into force on 1 September 2026. The consultation on the draft guidance in Chapter 3 closes on 10 September 2025. Any guidance would be published by the end of this year and apply from the same date as the new rule.

Separately, HM (His Majesty) Treasury and the FCA and PRA are reviewing the Senior Managers and Certification Regime. Consultation papers were issued in July 2025. This review of the SM&CR is not expected to impact the NFM proposals.

Key considerations for firms

Firms will need to agree a clear and consistent definition of NFM that can be applied within existing processes and policies; and consider approaches to determining where misconduct meets the threshold of "serious". While the FCA is consulting on guidance which would provide greater clarity on these matters, any guidance will not be exhaustive, and firms will need to exercise carefully considered judgment.

Assess policies and procedures in relation to identifying NFM. Firms should review current processes, practices and expectations in light of the changes, alongside the FCA's NFM survey findings issued in October 2024. The regulator has made clear that an inability to identify and tackle NFM is a warning sign of a failing culture and wants to give firms greater clarity and confidence to take action. The FCA expects firms to have robust processes, procedures and controls to detect NFM, facilitate appropriate outcomes and report relevant matters.

Review training for conduct rule staff and HR teams. This includes reviewing misconduct reporting and 'speak up' processes to ensure they are sufficiently robust and operate in a culture where these are used in practice. Firms may also need to revisit how existing HR and legal processes (e.g. disciplinary processes) are connected to these, to ensure that relevant issues are identified.

Reflect on the FCA's broader expectations on governance; risk management; preventing, investigating and reporting NFM; and inclusive cultures.

Non-financial misconduct (continued)

Internal Audit focus areas

01

Governance and accountability mapping

Review how the firm has embedded accountability for non-financial misconduct into governance frameworks, including Board and Senior Management Function (SMF) oversight. Verify whether NFM risks are clearly defined, owned, and reported within the governance structure.

02

Conduct Rules integration and SMCR alignment

Assess how Conduct Rules have been updated to reflect the FCA's expanded definitions, especially concerning bullying, harassment, and discriminatory behaviour. Confirm alignment with fitness and propriety assessments, disciplinary frameworks, and regulatory references.

03

Policies and disciplinary procedures

Test whether HR, whistleblowing, grievance, and disciplinary policies have been updated to reflect the regulatory changes. Check for consistency and completeness in escalation, documentation, and decision-making procedures.

04

Data sources and monitoring

Evaluate the breadth and depth of data sources used to detect and monitor NFM (e.g. whistleblowing, staff surveys, exit interviews). Validate whether reporting lines are clear, anonymous channels are effective, and MI is analysed with appropriate triggers for escalation.

05

Training and cultural change programmes

Review the design and delivery of training on NFM, ensuring it is role-relevant and tailored to evolving Conduct Rule obligations. Test how effectively these programmes are changing behaviours and supporting a speak-up culture.

06

Employee lifecycle risk controls

Assess controls over recruitment, onboarding, performance management, and promotions to ensure alignment with cultural expectations. Review how misconduct history is captured and factored into hiring and reference decisions.

07

Incident management and investigations

Review case handling of NFM incidents for fairness, timeliness, documentation, and independence. Confirm root cause analysis is conducted and lessons learned are captured and embedded.

08

Board reporting and cultural MI

Test the regularity, granularity, and insightfulness of culture-related MI presented to Boards and senior committees. Confirm whether culture indicators are triangulated across sources and tied to risk appetite.

Building organisational resilience to fraud

Fraud threats are rising, driven by ever-increasing digitalisation, the industrialisation of fraud by organised crime groups and criminal adoption of technology. New laws and regulation in the UK bring a fresh legal and compliance perspective, alongside longstanding commercial and reputational risks. IA should assess how fraud defences are evolving to address the changing risk landscape.

Fraud continues to be a strategic risk area for all organisations regardless of sector. The nature of the threat is changing rapidly, and businesses must respond with urgency and adaptability.

The following highlights three key areas of concern in organisations:

Insider Threat: Organised criminal groups are increasingly targeting employees through coercion to infiltrate the organisation and to facilitate fraud from within. Insider threat assessment and risk mitigation measures may not be keeping pace.

ECCTA Readiness: The new 'failure to prevent fraud' offence introduced by the Economic Crime and Corporate Transparency Act ('ECCTA') came into force on 1 September 2025. This new regulation focuses on fraud where the organisation or its clients derives benefit from the fraud being perpetrated by an associated person. Organisations should have considered the impact of the new law and whether risk mitigation measures are aligned to the 'reasonable procedures' guidance. Our recent publications on ECCTA provide more detailed guidance on this: ECCTA, what happens next; Insights, ECCTA: Failure to prevent fraud

Business-targeted scams: Sophisticated frauds using deepfakes and voice cloning are targeting high-value business transactions. These scams exploit human trust and system gaps and place further pressure on controls over payments. Updates to awareness training, payment controls and escalation protocols may be needed.

Key considerations for firms

Insider Threat

- Regular insider risk assessments should be in place, supported by a strong ethical tone and attention to cultural drivers such as low morale or pressure, with speak-up mechanisms that are effective and trusted.
- Use of behavioural analytics and clear escalation protocols are useful tools to help organisations to identify and respond swiftly to anomalies or collusion.
- As fraud risks become more complex, it is imperative that organisations regularly align and review access rights, prevent privilege creep, and maintain segregation of duties. It is good practice to seek assurance that excessive access risks are effectively mitigated.

ECCTA Readiness

- Formal governance structures and defined ownership should be established for ECCTA compliance, with Board-level visibility and regular reporting to demonstrate progress against the 'failure to prevent fraud' offence.
- Fraud prevention and detection controls should be risk-based, proportionate, and formally documented.
- Data-driven detection techniques and third-party due diligence are key anti-fraud measures, and their effectiveness should be regularly reviewed.
- Clear responsibilities across all levels can be reinforced through tailored training, scenario-based exercises, and ongoing fraud awareness, including how to recognise and address risks from associated persons.

Business-targeted scams

- Robust verification processes for payments and high-value approvals help mitigate the risk of manipulation, particularly where voice, email, or video instructions could be exploited. Effective safeguards reduce susceptibility to social engineering.
- Training key staff to detect AI-enabled impersonation threats - supported by simulation exercises and case reviews - strengthens organisational preparedness. Extending awareness beyond control functions to operational teams ensures resilience is embedded more widely.
- Advanced monitoring tools that use external data, entity resolution, and AI can enhance detection of evolving scams. Clear, rapid escalation mechanisms for suspicious activity are an important part of an effective response framework.

Building organisational resilience to fraud (continued)

Internal Audit focus areas

01
Governance and accountability

- Review the governance and ownership of fraud risk management, including clarity of accountability, programme sponsorship, and visibility at Board level.
- Assess whether ECCTA compliance is being actively managed, with progress reporting and oversight structures in place that demonstrate compliance with guidance on the "failure to prevent fraud" offence.

02
Culture and awareness

- Evaluate how fraud risk awareness and ethical culture are embedded across the organisation, drawing on sentiment indicators, stakeholder feedback, and the effectiveness of speak-up mechanisms.
- Examine escalation processes to determine whether responses to suspected fraud are timely, clear, and well-coordinated across functions.
- Assess the adequacy of fraud training, testing whether programmes are tailored by role, reinforced through simulations and case studies, and effective across both frontline and controls functions.

03
Prevention and detection

- Evaluate the adequacy of fraud prevention and detection procedures, ensuring they are proportionate, risk-based, and documented, and that ECCTA-specific risks are addressed.
- Inspect governance and controls over access to systems, including oversight of user privileges, prevention of privilege creep, segregation of duties, and use of anomaly monitoring to detect irregular activity.
- Test verification controls over payments, account changes, and approvals for resilience against manipulation, including AI-enabled impersonation techniques such as deepfakes and voice cloning.

Market Abuse and Surveillance

The implementation of Market Abuse Surveillance controls within financial services firms are an important element in ensuring the that trading is conducted in a fair and effective manner preserving orderly markets.

Key regulatory actions in recent years

2019 – Cross-**product manipulation, €20 million:**

The French regulator AMF alleged that a firm had been manipulating the price of French/Belgian bonds across different instruments and asset classes.

2024 – Venue detection, $348.2 USD million:

The US regulator CFTC fined a firm for failure to monitor trading activities due to incomplete data feeding surveillance platforms and a lack of adequate data controls.

2024 – Pre-trade control failures, £61.6 million:

The FCA and PRA both fined a firm for failing to have the adequate controls and real time monitoring needed to prevent an erroneous, large order from being entered into the market. The order caused a short-term drop in some European indices.

2024 – Suspicious orders, $4.9 AUD million:

The Australian regulator ASIC fined a firm for failing to prevent suspicious orders being placed in the electricity futures market. It was noted that the cause of the failure was a lack of appropriate systems to prevent and detect suspected manipulation.

Key themes and insights that are influencing evolution of surveillance functions

Cross-Product Manipulation

Cross-product manipulation involves deliberately influencing the price of one financial instrument to affect the value of another.

Traditionally, surveillance frameworks have focused on individual products. Detecting cross-product manipulation requires firms to adopt new approaches: including understanding inter-product relationships, redesigning monitoring logic, and often investing in enhanced technology to implement suitable cross-product controls.

Establishing or enhancing such capabilities typically demands a significant level of subject matter expertise, resourcing, and funding. Many firms still lack the coverage needed to withstand regulatory scrutiny.

Model Risk Management

Surveillance functions are increasingly being brought within the scope of broader Model Risk Management (MRM) frameworks. As surveillance systems, particularly those using algorithmic logic or AI become more advanced, they are more likely to fall under the definition of a "model" as defined by firmwide policy or regulatory guidance.

Integrating surveillance into existing MRM governance can introduce several challenges, especially where these systems have historically operated outside formal model oversight structures. These challenges can include inconsistent and incomplete documentation, unclear ownership, and evidencing model functionality. Vendor tools can present “black box” challenges around how a model functions.

The regulatory bar is rising for explainability and model performance in compliance-critical functions. There is growing scrutiny over governance blind spots, particularly where surveillance tools fall outside of formal model inventories or have not undergone independent validation.

Data Governance & Controls

Effective surveillance relies on timely, complete, and accurate data drawn from a wide range of structured and unstructured sources. Examples of necessary data include: trade, order, communications, market, and HR data.

Regulators expect firms to have implemented a robust data governance framework, through which they manage, validate, and maintain data integrity.

We have observed that data lineage and relevant controls are often poorly documented, and whilst most firms have controls in place to monitor data delivery and timeliness, there often exists a control gap relating to the validation of the data's completeness and accuracy.

We have additionally seen failings relating to the governance of issues. The raising and remediation of data issues must be tracked, documented, and reported on to relevant stakeholders and governance forums.

Market Abuse and Surveillance (continued)

Emergence of Artificial Intelligence

AI is increasingly shaping the way Compliance functions detect and manage risk behaviours. While it presents significant opportunities, its adoption also introduces new challenges that firms must address with care.

In market abuse surveillance specifically, AI has seen the most tangible progress in communications surveillance. Improvements in speech-to-text technology have enabled voice data to be treated similarly to other communication channels. Enhanced translation capabilities have reduced reliance on specialist language support and improved interpretation accuracy. The use of large language models (LLMs) has led to more targeted and productive alerting, reducing volumes of false positives and improving analyst efficiency.

In trade surveillance, AI presents the potential to detect more sophisticated forms of abuse - including complex patterns of cross-product manipulation - by learning from historical data and identifying behavioural anomalies beyond the reach of traditional rules-based systems. AI can also be applied to the efficient handling of false positive alerts, using pattern recognition and predictive modelling to identify and close these alerts automatically.

However, the application of AI also brings increased scrutiny from a model risk management perspective. As AI models grow more complex, firms must ensure clear documentation of model inputs, outputs, assumptions and limitations. The explainability of AI-driven decisions, particularly those influencing surveillance alerts, is essential - not only to satisfy governance and regulatory expectations, but also to maintain trust in the outputs.

The success of AI in surveillance depends on the quality and integrity of the data it consumes. A clear lineage from source systems to model input is critical, along with robust validation of the datasets used to train or inform AI tools.

Key considerations for firms

Firms must have effective systems and controls over both trading activity and trader communications, enabling timely detection, escalation and reporting. At the core of a strong surveillance framework is the Market Abuse Risk Assessment (MARA). This should demonstrate a firm's understanding of its risk landscape; identify in-scope products, activities and data; assess inherent risks; and evaluate control effectiveness to determine residual risk - reflecting where the likelihood and impact of abuse remains. This risk-based approach should inform the design and operation of the Surveillance programme, which typically comprises several key components:

Governance: The Surveillance programme should operate under strong and transparent governance, covering both BAU processes and strategic enhancements. Roles and responsibilities, including accountability for Surveillance outcomes, must be clearly defined.

Scenario and model inventory: A comprehensive record of all scenarios and models should be maintained and aligned to the MARA. Documentation should be kept up to date, especially for models leveraging AI or machine learning.

Control effectiveness reviews: Surveillance coverage should be reviewed regularly in light of changes in trading patterns, market structure or regulatory expectations. These reviews should lead to tangible improvements and refinements in controls.

Technology and automation: Surveillance tools - including scenario engines, alert generation platforms and case management solutions - must be well maintained, scalable, and capable of adapting to future business or regulatory changes.

Data governance: Surveillance-relevant data must be provided in a timely and secure manner. There should be clear checks in place to ensure the quality and completeness of all ingested feeds, alongside a documented understanding of end-to-end data lineage.

Management information: MI should enable senior stakeholders, both within and outside Surveillance to understand the status of controls, risks and open issues clearly and concisely.

Market Abuse and Surveillance (continued)

Internal Audit focus areas

01

Trade Surveillance Controls (including cross-product risk): Assess whether the surveillance framework is designed to detect market abuse across relevant asset classes. This includes traditional single-product surveillance as well as more complex cross-product manipulation. IA should review the product scope, use of automation, and whether scenario logic reflects known and emerging abuse typologies.

02

Communications Surveillance: Evaluate the scope and effectiveness of communications surveillance across all relevant channels, including email, chat, voice and messaging platforms. Consider the application of transcription and translation tools, the use of AI for alert generation, and whether alert handling and escalation procedures are effective and well documented.

03

Risk Assessment Coverage: Confirm whether the Market Abuse Risk Assessment (MARA) includes risks relevant to both trade and communications surveillance. This should include cross-product scenarios where applicable. IA should assess how product relationships are defined, the rationale documented, and whether the risk assessment is refreshed regularly and used to inform surveillance design.

04

Documentation and Escalation Procedures: Review whether procedures for investigating alerts are clearly documented, regularly updated, and reflective of operating practices. Confirm that control ownership and escalation pathways are clearly defined and consistently applied by analysts and supervisors.

05

Model Governance and Inventory: Verify that all in-scope surveillance models - including vendor tools and Artificial Intelligence/Machine Learning-based solutions - are captured in the firm's model inventory and subject to Model Risk Management (MRM) oversight. Check that documentation, classification, and review timelines are in place and adhered to.

06

Model Testing and Validation: Assess whether model testing is conducted and evidenced at appropriate intervals. This includes back-testing, performance metrics, and explainability testing. Where external models are used, confirm the level of transparency available and whether validation is independently performed.

07

Data Governance Controls: Audit the completeness of data lineage documentation, with control points identified from source systems to surveillance outputs. Confirm whether field-level mapping has been conducted and whether automated controls validate data quality, accuracy, and completeness.

08

Management Information (MI) and Escalation: Review the quality and timeliness of MI provided to governance forums and control owners. IA should check whether data issues and control exceptions are escalated promptly, tracked effectively, and remediated with accountability.

Digital assets

The UK Government and authorities are developing a comprehensive digital assets framework and actively engaging with the industry to position the UK as a global leader in digital finance. The FCA is expected to publish its cryptoasset regulatory framework mid-2026.

The UK is laying the groundwork to become a global centre for digital assets, with a clear regulatory roadmap. The FCA's new framework will cover cryptoassets and fiat-backed payment stablecoins, as well as authorisation, issuance, trading, custody, market abuse and prudential obligations. Final policy statements are expected in mid-2026, with the regime and new rules taking effect in early 2027.

In parallel, the BoE and PRA are building prudential treatment of banks' exposures to cryptoassets, and expectations for systemic stablecoins, including rules on backing, redemption, and oversight. The Government has signaled strong support for digital assets, recognising their role in innovation and market evolution. It continues to back stablecoins, tokenisation and broader use of distributed ledger technology across financial services. Key initiatives include the Digital Securities Sandbox, enabling real-world experimentation, and the first pilot for digitally native UK Government bonds (digital gilts).

The UK is developing its digital assets regime at a measured pace, while the EU, US, Hong Kong, Singapore and Dubai have introduced frameworks. To support market participants and remain competitive, the UK needs to keep up with the momentum.

See below links to further resources relevant to this topic: PwC's Global Crypto Regulation Report 2025; and PwC's Global FS Crypto Services site.

Key considerations for firms

Client demand and product development: Firms should assess opportunities to offer new products and services, including structured products, funds, Exchange-Traded Products (ETPs) or trading access linked to cryptoassets and tokenised assets, responding to growing retail and institutional demand as well as global regulatory clarity.

Stablecoins and digital money: Firms should evaluate use of fiat-backed stablecoins and tokenised deposits for internal treasury, cross-border payments, and on-chain settlement across business lines, in-line with the BoE's expectations.

Tokenisation and infrastructure: Firms should explore issuing tokenised assets or funds, participating in tokenised trading venues, or integrating with distributed ledger infrastructure to enhance efficiency and reach. Firms should consider opportunities to engage with the UK Digital Securities Sandbox, monitor global initiatives led by the BIS, and track the FCA's evolving regulatory approach to tokenisation.

Risk, compliance and governance: Firms should align risk, legal and compliance frameworks to support digital asset activity, and ensure executive and Board-level ownership as regulation evolves.

Strategic positioning and partnerships: Firms should identify where to build, partner or invest, such as in custody, wallet infrastructure, token issuance platforms or compliance technology.

Client engagement and controls: Firms should develop clear digital asset disclosures, onboarding flows and suitability processes, particularly where products are targeted at retail or wealth clients.

Digital assets (continued)

Internal Audit focus areas

Regulated firms already involved in, or preparing to enter the digital assets space, should ensure IA is ready to provide timely assurance ahead of the UK regulatory framework implementation.

01

Regulatory change impact

Plan assurance over the firm's response to upcoming UK regulatory changes, including how FCA, BoE and PRA expectations are being tracked and embedded into business planning.

02

Control design and effectiveness

Test whether existing risk and control frameworks adequately cover digital asset activities, including custody, trading, stablecoin use, and tokenisation projects.

03

Governance and accountability

Review governance arrangements to confirm clear ownership, escalation routes and oversight for digital asset initiatives at executive and Board levels.

04

Third-party and outsourcing risk

Test controls around the selection, onboarding and monitoring of external partners involved in custody, wallet infrastructure, blockchain platforms or token issuance.

05

Product governance

Assess design, approval and review processes for cryptoasset and tokenised products, including risk assessments, legal input and compliance sign-off.

06

Data integrity and reporting

Evaluate the accuracy and reliability of data supporting digital asset operations and reporting, such as pricing feeds, blockchain records and reconciliation processes.

07

Client outcomes and disclosures

Review disclosures, onboarding and suitability processes to test whether digital asset products are marketed and sold in line with regulatory expectations and client understanding.

Fair Value / Product Governance

The FCA has conducted thematic reviews of the approach taken by general insurance (GI) and pure protection firms in relation to product governance, mostly recently in Summer 2024. The FCA recognises the steps that firms have taken to strengthen their approach to product oversight and governance arrangements; however, they highlighted that there are still some improvements required across the market to address shortcomings. These include but are not limited to: the quality of fair value assessments, senior manager accountability and the impact of distribution costs on product value.

In 2021, the FCA strengthened their Product Governance Sourcebook ('PROD') which applies to GI and protection businesses, including a requirement for insurance firms to ensure that their products are providing fair value to customers in their target market. The concept of product value was also introduced as part of the the Consumer Duty for other firms in 2023 but does not replace PROD where it applies.

The FCA has undertaken thematic reviews of firms' approaches to product governance for general insurance and pure protection products. The most recent review, conducted during Summer 2024, focused on whether firms could demonstrate that products & services are offering fair value to customers, that effective governance arrangements are in place and that action has been taken where value concerns have been identified. As part of their findings, the FCA recognised that firms had taken steps to strengthen their product oversight and governance arrangements, however, improvements were still required to address the shortcomings and inconsistencies across the market. Their headline findings related to product manufacturers not adequately assessing and being able to evidence that their product provides fair value. They also found that distributors did not fully understand their responsibility to consider how remuneration arrangements interact with both the benefits provided to the customer and to the overall product value.

We have already seen the FCA focus in where they have concerns surrounding product value, such as GAP insurance and premium finance. It is therefore paramount that firms ensure that their product oversight and governance arrangements are both appropriate and sufficient to be able to assess whether their products are providing value to customers in the target market.

Key considerations for firms

The list below provides a summary of key themes identified by the FCA, but is not intended to be an exhaustive list:

- Firms should ensure that their product oversight and governance frameworks are sufficiently robust to assess whether a product is providing fair value to customers in the target market.
- Distributors should ensure that they fully understand their distribution costs, including the impact on product value.
- Ensure that senior managers are aware of their responsibilities to provide real challenge on product value and exercise appropriate levels of challenge.
- Firms should take appropriate action when they identify that a product may not be providing fair value to customers, or where concerns arise regarding product value and/or poor customer outcomes.
- Management information should be relevant and of sufficient quality to support decision making and permit the firm to monitor customer outcomes.
- Both manufacturers and distributors should ensure the timely sharing of information up and down the distribution chain, including conclusions on product value.
- Manufacturers and distributors should ensure that their distribution strategies for each product are aligned to and meet the requirements of PROD.

Fair Value / Product Governance (continued)

Internal Audit focus areas

01

Policy and framework review

Review product governance and oversight frameworks (including a review of Product Oversight and Governance Policy) to ensure this is sufficiently robust, with appropriate escalation points where value and/or poor customer outcome concerns are identified.

02

Responsibilities

Ensure that committee terms of reference and SM&CR documentation are sufficiently clear on roles and responsibilities of senior managers with regards to product value and good customer outcomes.

03

Quality of fair value assessments

Product manufacturers should consider a review of fair value assessments completed by distributors to ensure they are compliant with the requirements under PROD and are sufficiently detailed to be able to assess product value.

04

Management information

Review existing MI dashboards to ensure that metrics that are being used are appropriate and effective to measure customer outcomes.

05

Remuneration arrangements

Both manufactures and distributors should consider a review of the distribution costs and ensure that these are reflective of actual costs incurred and are not having a detrimental impact on product value.

Consumer Protection and Premium Finance

In July 2025, the FCA published the interim findings of its premium finance market study. The market study was undertaken due to concerns the FCA had about the interest charged in this area. Whilst the FCA has specified that it does not intend to undertake specific market-wide interventions, they have specified their intention to use their powers up to and including enforcement where necessary. Firms should review the FCA interim report and prepare for the next phase of the market study.

On 22 July 2025, the FCA published their much-anticipated interim findings of their premium finance market study which took place in Q4 2024. The FCA had highlighted their concerns surrounding the value provided by premium finance products, with some APR levels in the market exceeding 30%. The FCA also expressed concerns regarding competition in the market and 'double dipping' where firms charge more for the insurance premium due to the credit risk of monthly payments, in addition to the cost of premium finance.

The main takeaways from the FCA's publications were:

- The interim report showed a tonal shift to being more focused on specific elements of Consumer Duty and PROD at a firm or market sub-set level rather than market wide changes. It is clear the FCA listened to challenges raised by firms and understood the range of models in the market and accepted there are costs to these.
- There are no plans to ban commission, enforce 0% APRs or prevent the sale of premium finance across the market. However, the FCA has expressed their intention to use their powers of intervention where they have concerns about profit levels or fair value which could include supervisory or enforcement action on individual firms.
- Whilst the FCA recognises that it does cost firms money to deliver the premium finance product to customers, they do still believe some firms are making too much profit in this area.
- 20% of the market are paying APR levels that are more than 30%, which is a level the FCA has previously expressed they consider to be high.
- Next steps will be for the FCA to focus on the higher APRs in the market and any subsequent intervention and/or enforcement action will be taken on a firm-by-firm basis.

Key considerations for firms

Firms should review the FCA interim report and prepare for the next phase of the market study.

Reflect on any APRs over 30% on premium finance and whether these can be justified ahead of the next stage of the premium finance market study.

Firms that are approached by the FCA to participate in the next phase of the market study should prepare their explanations as to why their APRs are above 30%.

Reflect on the profit made on premium finance products and whether this is reflective of the costs incurred to deliver the product to customers.

Consider whether the overall approach to the distribution of premium finance meets the requirements of Consumer Duty and PROD.

The FCA has said that they will use their powers up to and including enforcement where they consider firms are not meeting their current requirements on Consumer Duty and PROD.

Firms should review their current pricing strategy to ensure that there is no element of 'double dipping' occurring in relation to credit risk across both the insurance premiums and the premium finance.

Consumer Protection and Premium Finance (continued)

Internal Audit focus areas

01

Alignment with regulatory requirements and Fair Value Principles

- Product governance framework - Assess whether the firm's product governance framework and practices operate in line with relevant regulatory requirements, including PROD and the Consumer Duty.
- Fair value across the lifecycle - Evaluate whether fair value considerations are consistently embedded across the product lifecycle, and whether oversight mechanisms (e.g. committees, reviews) provide sufficient assurance that customer outcomes are prioritised.
- Premium finance focus - For a deep dive specifically on premium finance, review the firm's Fair Value Assessments (FVAs) for premium finance products. In particular, assess whether APRs above 30% are sufficiently justified, taking into account a range of factors (e.g. cost of funds, distribution arrangements, customer risk profile) and whether they provide fair value to customers.

02

Double dipping risk

- Assess whether the firm's current pricing methodology could result in customers being charged twice for credit risk (across both the insurance product and associated premium finance). Understand whether there are controls in place to prevent this and assess their effectiveness.

Valuation of Private Assets

The FCA's review of private asset valuations signals growing regulatory scrutiny as private markets expand. Inconsistent practices around governance, independence, and conflict management pose real risks. Firms must now treat valuation as a strategic priority: embedding robust and transparent processes to protect investor outcomes and support long-term confidence in an increasingly systemically important market.

In March 2025, the FCA published the results of its review of private market valuations. The review was a comprehensive multi-firm assessment focusing on how private market asset managers determined asset values.

This initiative was driven by the rapid growth of private markets and increasing exposure of UK investors, both institutional and retail, to such assets. Given the inherent opacity, subjectivity, and illiquidity of private market investments, the FCA sought to ensure that valuations are fair, consistent, and transparent, especially under stressed market conditions.

The review covered a range of asset types and engaged with a broad sample of market participants. It assessed governance arrangements, conflicts of interest, independence, policies and procedures, frequency and disclosure of valuations, use of methodologies, and third-party oversight. The overarching goal was to identify good practices and highlight deficiencies that could threaten market integrity, investor confidence, and regulatory compliance.

The FCA emphasised that robust valuation practices are foundational to investor protection, risk management, and market integrity. Valuations underpin critical activities such as fee calculations, asset transfers, fund subscriptions/redemptions, and borrowing (e.g. Net Asset Value (NAV) -based financing), making deficiencies in valuation processes a potential source of significant harm. The review also acknowledged global interest in this issue, referencing recent work by IOSCO (International Organisation of Securities Commission) and the Bank of England on the systemic risks posed by opaque and inconsistent private market valuations.

While many firms showed good practices, the FCA highlighted inconsistencies in conflict management, methodology application, and ad hoc valuation processes. These gaps pose risks to investor fairness, financial reporting, and market integrity, especially as private markets grow in size and complexity.

Valuation is no longer a niche control issue, it is a strategic risk. Firms should move beyond compliance to embed robust, transparent, and independent valuation frameworks. As regulatory expectations evolve, proactive governance will be key to building trust and sustaining growth in private markets.

Key considerations for firms

Governance and Oversight - The FCA identified varying effectiveness in governance structures. Issues included insufficient independence of valuation functions and weak committee challenge. Firms should demonstrate independence, clear responsibilities, and valuation decisions that are appropriately scrutinised and documented.

Conflicts of Interest - Conflicts arose where valuation outcomes could impact performance fees, remuneration, or investor treatment. Firms need to identify, manage, and clearly disclose such conflicts, and ensure marketing and governance materials reflect them.

Valuation Policies and Methodologies - Policies often lacked detail, were outdated, or inconsistently applied. Methodological shifts were sometimes poorly justified. Firms need well-documented, consistent, and rational valuation frameworks aligned with asset type and risk profile.

Frequency/Disclosure - Valuation frequency varied across asset classes e.g. quarterly for private equity and monthly for infrastructure equity, while some firms relied on ad hoc valuations. Valuation cycles should be regular and risk-sensitive, with improved transparency around NAVs, asset-level values, and methodology disclosures.

Third Parties - External valuation support was common but used inconsistently. Some firms delegated too heavily without sufficient internal oversight. The FCA expects firms to retain accountability, critically assess external inputs, and avoid overreliance on advisers.

Employee Remuneration - In some cases, staff responsible for valuations had performance-linked pay, creating potential bias. Firms should decouple valuation responsibilities from variable remuneration tied to fund returns to avoid undue influence on valuation outcomes.

Valuation of Private Assets (continued)

Internal Audit focus areas

01

Governance

Confirm that valuation oversight structures - such as committees are independent, clearly mandated, and actively engaged. Assess whether roles are well-defined and whether decision-making is appropriately documented. Consider adequacy of skills and capacity.

02

Conflicts of Interest

Check that potential conflicts (e.g. fee structures, investor class preferences) are identified, assessed, and effectively mitigated. Disclosures should be accurate and aligned across policies, offering documents, and marketing materials.

03

Valuation Policies

Ensure that valuation policies are up to date, comprehensive, and applied consistently across similar asset types. Any changes in methodology should be well-justified and supported by appropriate governance.

04

Frequency & Triggers

Verify that valuation frequency aligns with the nature and risk profile of the assets. Ad hoc or event-driven revaluations should be backed by clear criteria and documented rationale.

05

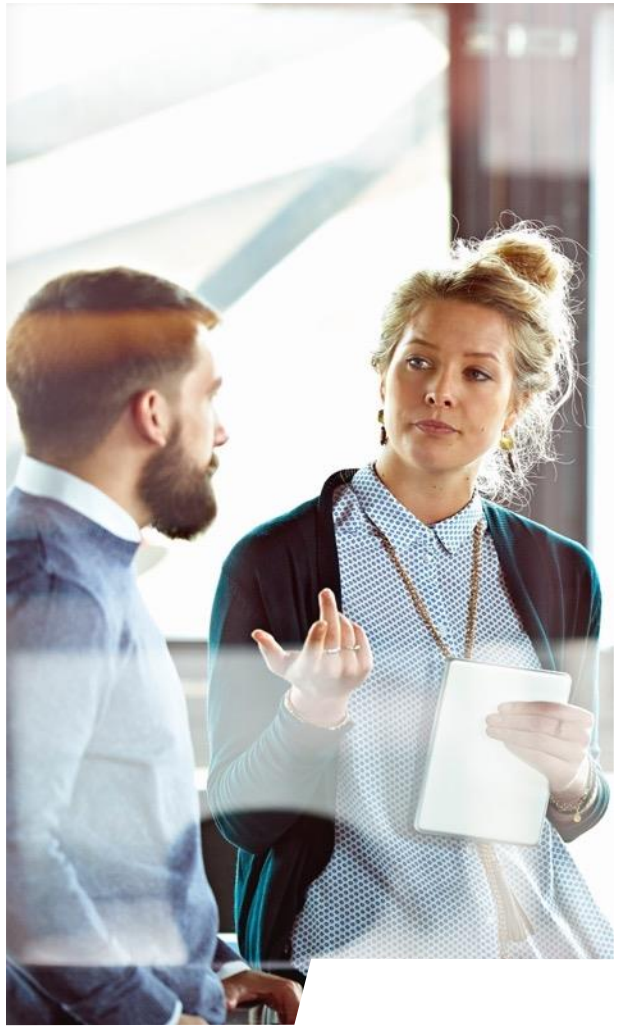
Third-Party Oversight

Assess whether external valuers are subject to appropriate due diligence, selection criteria, and performance review. Firms should retain responsibility for final valuation decisions and not default to external opinions without scrutiny.

06

Remuneration

Confirm that staff involved in valuations are not subject to incentive structures (e.g. carry or performance fees) that could compromise independence. Review the extent to which remuneration frameworks reinforce objectivity and segregation from portfolio management.



Advice guidance boundary review

The FCA and His Majesty's Treasury (HMT) are reshaping how firms support retail investors through the Advice Guidance Boundary Review. This landmark reform has the potential to reshape how consumers access financial support without triggering regulated advice, unlocking new opportunities for firms while demanding stronger governance, oversight, and risk management.

The Advice Guidance Boundary Review (AGBR) is a major initiative of the FCA and HMT to address the concern that too few consumers in the UK are receiving the help they need to make informed investment and pension decisions.

Under the current framework, HMT believes that firms have adopted a cautious approach to providing guidance, due to the risk of them tipping into providing regulated advice. This has contributed to an advice gap, leaving a significant proportion of retail investors underserved, particularly those with smaller portfolios or less complex needs; this has also hindered returns for consumers.

HMT and the FCA seek to deliver a new form of 'targeted support', enhance the uptake of 'simplified advice', and clarify the advice boundary. This will enable firms to offer new services. The two main proposals are:

- Targeted Support: Outcomes for groups of similar consumers based on shared characteristics (e.g. nudges to invest surplus cash or avoid unsustainable pension withdrawals).
- Simplified Advice: Streamlined personal recommendations for consumers with limited, well-defined needs (e.g. investing a lump sum).

The initiative is also designed to support the UK's long-term economic growth by improving retail participation in capital markets and long-term saving. The FCA sees this as key to ensuring that consumers can access appropriate products and services and that financially excluded individuals are not left behind. Firms will be expected to deliver and evidence fair value and good outcomes, even where customer support does not take the form of regulated advice.

FCA's key timeline

- Consultation for targeted support and simplified advice, closed on 29 August.

- Authorisations window for new targeted support permission opens in October 2025.
- Finalise the regulatory framework and publish a policy statement on targeted support in December 2025, and a consultation on simplified advice in January 2026.

- Work continues to consolidate, simplify and clarify the FCA's guidance on the advice boundary during 2026.

Advice guidance boundary review (continued)

Key considerations for firms

Decide whether targeted support is a strategic opportunity - Firms wishing to deliver targeted support will need to apply for an additional permission from the FCA, with the regulator then reviewing the firm's processes and controls. If firms decide to commence this service, then they will need to:

Redesign customer journeys: Firms should review how digital and hybrid engagement models can help deliver clearer, more accessible pathways for consumers to receive appropriate guidance or advice. This includes ensuring that customer journeys support good outcomes without straying beyond the regulatory boundary. Where new tools or support models are introduced, they should be subject to a risk assessment, with appropriate governance, monitoring, and escalation procedures to evidence fair value and consumer protection.

Govern segmentation and targeted prompts: Firms must ensure that segmentation logic used for 'targeted support' is fair, evidence-based, and free from unintended bias or exclusion. Boards should challenge how these customer groupings are defined and how their use aligns with conduct, vulnerability and inclusion responsibilities.

Embed outcomes monitoring and MI dashboards: Management should ensure that real-time monitoring of outcomes, particularly for targeted or simplified journeys, is embedded into risk and conduct reporting. This includes reviewing KPIs for vulnerable customer groups, complaints, and any emerging conduct issues arising from "guidance-led" customer experiences.

Internal Audit focus areas

01

Oversight of Advice vs Guidance Frameworks

IA should check that new processes clearly separate regulated advice, simplified advice, and targeted support, and that these stay within the FCA's rules. IA should test the controls surrounding how this works in practice - for example, whether staff use scripts consistently, use digital tools correctly, and avoid giving advice when only guidance or support is intended.

02

Disclosures and record-keeping in support journeys

IA should assess whether disclosures, risk warnings, and records support good customer outcomes in non-advised and simplified advice journeys. The focus should be on how consumers understand and act on the information provided, rather than whether standard wording is in place. Testing should consider whether the end-to-end journey leads customers to the right outcome in practice.

03

Governance of targeted support models

IA should carry out a root-and-branch review of how targeted support models are being developed and implemented. This includes assessing whether the design, governance, risk assessment, and controls are operating effectively, and whether they operate within the FCA's rules. Testing should look at the end-to-end process, from how targeted support is designed and approved, to how it is delivered to customers, monitored, and escalated when issues arise.

04

Controls over digital tools and AI models

Where AI, robo-guidance or algorithmic prompts are used, IA should review model risk governance, validation procedures, and outcomes testing. Controls should ensure explainability, human oversight, and compliance with evolving FCA expectations. Effectiveness should be verified by reviewing testing logs, model behaviour, and incident handling (e.g. override or drift events).

Solvent exit planning (continued)

The PRA is strengthening expectations around insurer market exits through PS20/24, requiring firms to plan for a solvent exit as part of business-as-usual activities. This aims to ensure insurers can exit the market in an orderly way without triggering insolvency or relying on formal resolution, enhancing stability and protecting policyholders.

In the last few years, the PRA has said it plans to increase confidence that insurers can exit the market with minimal disruption, in an orderly way, and without having to rely on the backstop of an insolvency or resolution process. In December 2024, the PRA published Policy Statement PS20/24 on Solvent Exit Planning for Insurers, setting out new requirements to enhance the UK insurance sector's preparedness for orderly market exit.

PS20/24 requires in-scope insurers to prepare exit plans, to a level of detail commensurate with their size and impact. The aim is to ensure a smooth and efficient exit for insurers while protecting policy holders.

Who does it apply to?

- UK Solvency II firms
- UK Non-Directive firms
- Society of Lloyd's
- Mutuals and Friendly Societies
- Run-off acquirers

While the rules do not apply on a group-level basis, solo insurers should consider the implications and risks arising from group membership and are expected to assess any group-wide risks or dependencies that may impact their ability to exit in an orderly manner.

Key considerations for firms

PRA Requirements

- PS20/24 includes new rules and requirements for insurers to prepare for a solvent exit and document their preparations in a solvent exit analysis (SEA).
- Insurers would also need to prepare a detailed solvent exit execution plan (SEEP) if a solvent exit becomes a reasonable prospect.
- Insurers need to prepare a SEA as part of their business as usual activities, and update it at least every three years.

The rules come into force on 30 June 2026. In-scope entities are expected to have taken their SEA through their internal governance processes i.e. presented and discussed with the Board by 30 June 2026.

PRA expectations

In addition to the mandatory requirements, the PRA sets out expectations to guide implementation and ensure consistency with existing regulatory regimes:

- Work undertaken under existing recovery and resolution requirements should be drawn upon so that new solvent exit preparations are consistent with existing policies.
- These proposals go further than existing requirements: insurers should consider both the financial (e.g. capital) and non-financial resources (e.g. key staff) that they will need to execute a solvent exit effectively.
- Boards should be engaged on recovery and resolution requirements and ensure they scrutinise and challenge solvent exit preparations.
- Insurers should determine criteria for when solvent exit becomes a reasonable prospect, triggering a SEEP. This ensures firms are able to respond swiftly and appropriately when a solvent exit scenario arises.

Solvent exit planning (continued)

Key considerations for firms

H2 2024

Policy Statement released

Conduct gap analysis

Map existing documents against the SEA requirements.

Identify where further work may be required, or inconsistencies addressed.

Produce SEA

Produce the SEA to meet the requirements of the changes.

Plan to refresh the SEA on a minimum 3 yearly cycle

June 2026

Implementation

Review existing documentation

Gather existing documentation on recovery resolution, risk frameworks, risk appetite, financial models, communications plans and management actions.

Undertake remediations

Plan further modelling to fit with current production cycle

Amend and extend current resolution plans and risk monitoring.

Gain assurance

Undertake independent assurance activities alongside sufficient challenge from governance processes

Sources:

PS20/24 – Solvent exit planning for insurers | Bank of England
CP2/24 – Solvent exit planning for insurers | Bank of England

Internal Audit focus areas

As insurers work towards meeting the PRA's requirements for Solvent Exit Planning under PS20/24, IA has a role to play in providing independent assurance over the design, execution and governance of solvent exit arrangements. The following areas should form key pillars of IA's focus:

01 Remediation - Assessing whether remedial actions have been undertaken and completed following a gap analysis being conducted to map existing documents to SEA requirements. The PRA will expect that any material gaps are addressed at the time of implementation.

02 Independent Assurance - Undertaking independent assurance to ensure the firm's SEA meets the PRA's requirements and to assess whether sufficient challenge has been undertaken through the internal governance process. This will provide the PRA with additional oversight and comfort of insurers' solvent exit plans.

03 Assessment - Assess whether the process for undertaking a SEA is appropriate and whether SEA forms part of entities' compliance / audit planning. The SEA should be a regular exercise undertaken by entities to ensure they remain up-to-date and relevant to insurers' business models and strategies.

IA should ensure that solvent exit planning is not treated as a one-off compliance exercise, but rather as a well-embedded, risk-based process that is subject to regular oversight, testing, and challenge - ultimately contributing to the firm's operational resilience and regulatory readiness.

Treasury – Collateral and Liquidity Management

The PRA has renewed its focus on the liquidity risk management capabilities of insurers, emphasising the need for robust frameworks to withstand stress and uncertainty. Its consultation paper CP19/24 (December 2024) introduces new liquidity reporting templates, requiring c.3,000 data fields with up to 150 key metrics daily during periods of stress. The PRA is expected to issue its final policy statement in September 2025, with implementation set for June 2026, aiming to secure timely, consistent and comparable reporting, strengthening the PRA's supervision of liquidity risk across large insurers.

In recent years, insurers have faced increasing liquidity challenges as market volatility and economic uncertainty exposed weaknesses in risk management frameworks. Events such as the 2022 liability-driven investment crisis and subsequent collateral strains brought liquidity risk firmly into regulatory focus. The PRA has expanded its current regulatory regime around insurance liquidity, moving from the largely qualitative guidance in SS5/19 to more prescriptive requirements, set out in its consultation paper CP19/24 in December 2024. CP19/24 introduces new liquidity reporting templates for large insurers, requiring firms to capture detailed historical and forecasted data on cash flows, sensitivities / stresses and committed facilities.

The proposals seek to provide consistent, timely and comparable information, with around 3,000 data points to be reported on monthly / quarterly or annually, with flexibility for daily submissions during periods of stress. The PRA's action has brought liquidity risk to the forefront for insurers, with in-scope life firms now focused on meeting the upcoming reporting requirements and aligning their frameworks to comply with CP19/24. The scope is currently set by balance sheet size, derivatives and securities financing thresholds. To ensure successful operational readiness preparations, significant capability uplift is required across Treasury, Finance, Actuarial, Asset management and Risk / Compliance functions.

Key considerations for firms

Assess gaps against CP19/24 templates by reviewing prescribed data requirements, identifying where data is missing, incomplete or of insufficient quality across systems and processes.

Remediate identified gaps through targeted fixes in data sourcing, process enhancements and technology upgrades, ensuring firms can deliver timely and accurate reporting.

Prepare for upcoming PRA policy statement (September 2025) by monitoring clarifications and final requirements, and adjusting implementation plans to align with any changes in scope, timelines or expectations.

Enhance collateral and buffer management by testing adequacy under normal and stressed conditions, supported by improved forecasting and contingency planning.

Embed PRA-prescribed stresses into risk appetite frameworks, aligning metrics, limits, and escalation procedures with day-to-day liquidity management.

Drive cross-functional collaboration between Treasury, Finance, Actuarial, Asset Management and Risk / Compliance teams to ensure a holistic and consistent approach.

Treasury – Collateral and Liquidity Management (continued)

Internal Audit focus areas

01

Impact and gap assessment

Confirm whether firms have identified existing data, process and control gaps against capabilities required to operationalise production and submission of the PRA's prescribed templates.

02

Capability build & readiness planning

Ensure adequate capability build and operational readiness plans are established to address identified gaps, with key milestones, ownership and timelines aligned to achieve readiness by June 2026.

03

Liquidity framework and consistency

Review the efficacy of the existing liquidity risk management framework to ensure adequacy of activities upstream of reporting, and confirm consistent definitions and effective controls across liquidity risk appetite and limit setting, stress testing, management of liquid resources and monitoring and reporting across the group.

04

Buffers and collateral management

Assess the controls around the setting of adequate group-wide liquidity buffers and collateral management under both normal and stressed conditions, ensuring ability to demonstrate sufficient liquidity resources under the PRA-prescribed stresses.

05

Governance and oversight

Review the sufficiency of senior management involvement, the effectiveness of liquidity-related controls, and the frequency and quality of second line of defence reviews on liquidity operations. This will include design and significant enhancements on the regulatory submission sign-off processes to allow T+1 and T+10 turnaround.

Embracing InsurTech

Innovation and disruption are accelerating, presenting both strategic opportunities and control complexities as insurers experiment with emerging technologies. In insurance, this is increasingly AI-led, with InsurTechs focusing on customer interactions (e.g. reducing failure demand), underwriting (e.g. automated risk placement), and claims (e.g. automated triage).

InsurTech refers to the use of technologies to transform insurance processes, products and distribution models. Increasingly, this shift is AI-led: many InsurTechs now position themselves as AI firms, piloting and scaling use cases across the insurance value chain. Innovation is being driven both externally by startups and scale-ups, and internally through the transformation programmes and proof-of-concepts of established insurers and brokers.

InsurTech is responding to structural pressures across the sector: rising cost of capital, legacy friction, changing customer expectations, and tightening regulation. According to our "The Untapped Potential within the UK Insurance Market" report, there is a £50 billion revenue opportunity from disruption, with 30% of the life and pensions market expected to be disrupted by 2030. Global investment in InsurTech surpassed $3 billion in 2018 alone, highlighting the scale of capital backing innovation across the insurance value chain. Inaction is increasingly not an option as firms risk losing relevance and market share to more agile competitors.

Yet with innovation comes risk. Deploying new technologies, particularly at pace or without sufficient oversight, can lead to breaches, non-compliance, and vendor dependency. As firms increasingly partner with or acquire InsurTech providers to accelerate digital capability, they may introduce hidden integration risks, including incompatible systems, inherited control weaknesses, or cultural misalignment. At the same time, competitive pressure can push firms to deprioritise documentation, testing and regulatory engagement in the drive to implement new solutions, such as algorithmic underwriting or embedded distribution. In this context, risk often arises not from the technology itself, but from how quickly it is scaled, how effectively it is governed, and how well it is embedded into the firm's broader control environment.

Key considerations for firms

Challenge innovation strategy and align it to risk appetite: Organisations should assess whether their innovation ambitions are clearly defined, appropriately risk-assessed, and aligned to business strategy and appetite. Failing to innovate is a risk in itself. All InsurTech initiatives, whether internally developed, partnered or acquired, should be subject to governance standards that cover ownership, oversight and escalation.

Clarify uplift thresholds and integration expectations: Pilot activity should not bypass core controls by default. Define clear criteria for when a proof-of-concept or partnership must be brought under standard frameworks (e.g. model risk, third-party assurance, legal review, etc.). Where InsurTech providers are acquired or integrated, firms should plan for risks from inherited systems, operating models and cultural fit.

Anticipate the complexity of scaling: Innovations that perform well in isolation may create unforeseen issues at scale. Structured risk reviews should consider whether operational resilience, regulatory obligations, and control effectiveness can be maintained when InsurTech solutions are deployed more widely.

Embracing InsurTech (continued)

Internal Audit focus areas

01

Regulatory compliance and engagement

Map applicable FCA/PRA obligations for innovative products and services; embed requirements into proof-of-concept to production gates, and evidence proactive regulatory engagement on higher-risk initiatives with supervisory advice and actions tracked.

02

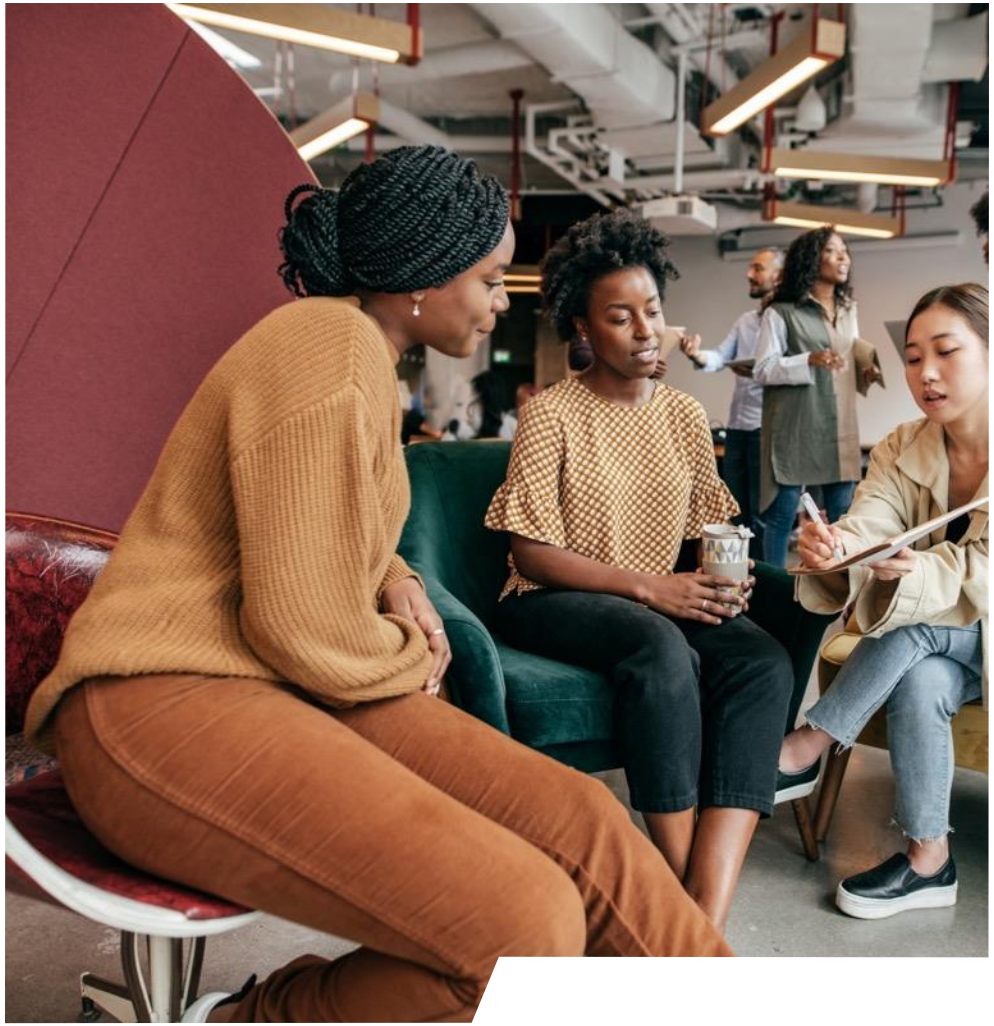
Third-party and vendor oversight

Validate lifecycle controls for InsurTech partners - due diligence, risk-based contracting (data, IP, audit, SLAs, exit), performance and concentration monitoring - and confirm tested exit and contingency plans for critical services.

03

Model and algorithmic controls

Verify governance over algorithmic underwriting, pricing and claims, e.g. documentation, explainability and bias testing, performance/drift monitoring, etc., with clear audit trails and oversight of third-party or hosted models and APIs.



Blueprint Two Phase One Readiness

A mandatory platform shift that demands technical readiness, operational alignment and cross-market coordination.

Blueprint Two is the multi-year programme to modernise Lloyd's of London, including its core infrastructure for premium and claims processing. Phase One replaces legacy systems, including CLASS (Claims Loss Advice and Settlement System), ECF (Electronic Claims File) and IMR (Insurers' Market Repository), with a new cloud-based platform. It introduces a shared gateway for structured messages, modern portals for premium and claims operations, and new orchestration and repository services. Participation in Phase One is mandatory for all market entities, including brokers, carriers and delegated authority participants, who must ensure onboarding to the platform in order to continue trading.

Phase One is focused on continuity rather than transformation. It provides the technical bridge to future automation by modernising infrastructure and access methods. Key services include the International Premium Orchestration Service (IPOS), International Claims Orchestration Service (ICOS), and the Document Repository Service (DRS). Market firms must also migrate messaging to the ASG Adept gateway, adopt new reporting via Qlik Sense, and update internal processes to reflect new portal and messaging-based interactions. These services apply across the market, however, the way they are used varies depending on the firm's role. For example, in the context of claims, brokers must submit claims messages (via LIMCLM messages or bordereaux through DRS) and supporting documents while insurers must retrieve and process claim transactions (responding to queries via ICOS or writeback depending on the setup).

At the time of writing, market testing will not commence before 2026. Due to earlier design choices, testing will need to be extensive to validate that the re-platforming delivers against market needs. Dress rehearsals and parallel runs will follow to provide assurance before final cutover. As a result, full re-platforming is not expected before 2028, and heritage systems will be maintained and supported until at least 2030 to provide long-term stability.

Key considerations for firms

Clarify ownership and oversight for Blueprint Two: Assign accountability for delivery, governance and readiness tracking. Ensure roles and responsibilities for adoption (including onboarding, process changes and user training) are clearly documented across business and technology teams.

Assess process and control impacts: Review impacted workflows, particularly where processes relied on legacy system notifications, bespoke messaging, or overnight batch runs. Examples include premium processing and query management within the claims process.

Develop and test data and messaging integration: Ensure technical readiness for messaging transitions, including the move from existing gateways to ASG Adept. Test supported messages, file collection locations and security authentication changes, and confirm fallback processes.

Decide on strategic versus minimum compliance adoption: Firms should determine whether to adopt only the mandatory requirements or use Phase One as a springboard to optimise processing efficiency, reduce manual workarounds, and align with their broader technology strategies to modernise core systems and integrations ahead of Phase Two.

Blueprint Two Phase One Readiness (continued)

Internal Audit focus areas

01

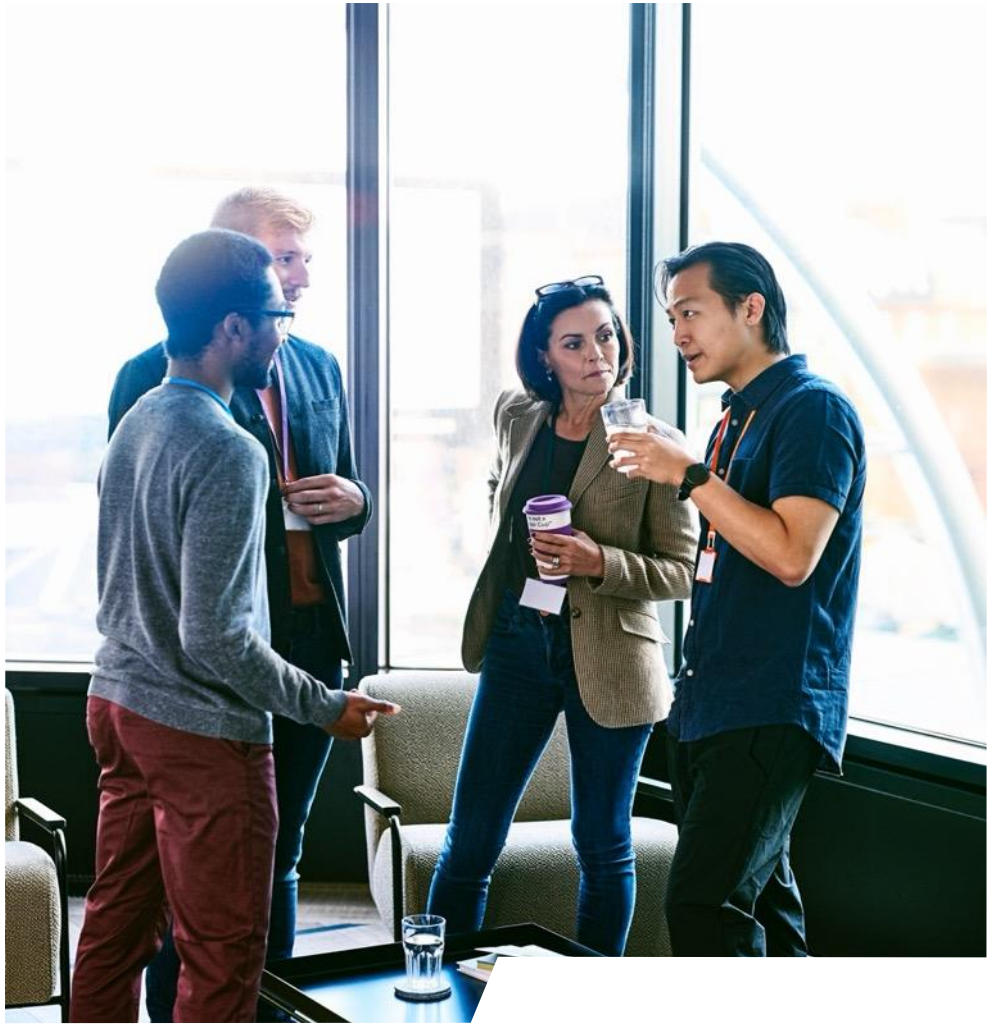
Assess Blueprint Two programme delivery and risk exposure

Review programme governance, risk management, and delivery milestones, including dependencies across technology, process and vendor change. IA should consider engaging technical specialists, such as PwC's Blueprint Two Readiness Assessment, to independently test programme controls and inform assurance over implementation readiness.

02

Evaluate operational preparedness for cutover

Confirm that systems, integrations and reporting capabilities have been tested, and that fallback plans are documented. Test whether process changes (e.g. claims handling, document upload, messaging) are reflected in updated procedures, training and control frameworks across affected business areas.



Internal Audit Practices and Capabilities

- Top of mind for CAEs
- Common challenges and early experience with the new Standards
- Preparing for EQAs under the New Standards
- AI in Internal Audit

Top of mind for CAEs

IA has always adapted to change, but the pace today feels different.

With both the IIA's Global IA Standards and the CIIA's IA Code of Practice taking effect in January 2025, attention is turning to how requirements should be interpreted, demonstrated in practice, and assessed through External Quality Assessments (EQAs) or readiness reviews.

At the same time, Boards and Audit Committees are raising expectations: they want sharper insights, broader coverage, and faster assurance - all against a backdrop of shifting risks from geopolitical uncertainty and cyber threats to climate change and organisational resilience.

For IA leaders, the question is no longer whether to broaden the remit, but how to do so without compromising independence or credibility. Drawing on recent EQAs, client experience, and market insights, we explore how functions are adapting: how technology, particularly AI, is enabling smarter assurance and sharper analytics; and how IA can evolve to meet higher expectations.

Ultimately, IA has a unique opportunity to redefine its relevance. By balancing conformance with value creation, driving functional evolution, and embedding responsible AI, it can position itself as a trusted partner that protects value while enabling resilience, innovation, and growth.

We frame our insights around three themes that are top of mind for Chief Audit Executives (CAEs) today

01

Common challenges and early experience with the new Standards: we share what we are seeing in practice as IA functions interpret the new requirements and work to demonstrate conformance. We also share our insights into leading practices, highlighting how functions that are ahead of the curve are embedding the Standards and Code.

02

Preparing for EQAs under the New Standards: we comment on the new four-point quality rating scale, what have we learned so far from our EQA experience and some helpful tips to prepare for your next EQA.

03

Adoption of AI in IA: we share insights on how emerging technologies can support smarter assurance, sharper analytics, and more compelling insights, while maintaining independence and responsible governance.

Common challenges and early experience with the new Standards

The Global Internal Audit Standards ('GIAS' or the Standards') and the CIIA's Internal Audit Code of Practice ('the Code') came into effect in January 2025. Together with the updated Quality Assessment Manual and the first Topical Requirements (starting with Cybersecurity), they reinforce the profession's aim to elevate IA's strategic positioning in organisations. While the intent is to drive consistency, maturity, and value creation; many IA functions are still working through how to interpret and evidence these requirements in practice.

01

Board and Senior Management Responsibilities (GIAS Standards Domain III; Code Principles 1–3) - focuses on governance and sets clear expectations for the Board and Senior Management.

Over the past year, many IA functions have struggled with how best to conform with and evidence the essential conditions relating to Board and Senior Management responsibilities.

Those that undertook readiness assessments early are now ahead: they have mapped each condition to their governance structures, built frameworks aligned to their business, and embedded these into day-to-day activity. In many cases, they have also actively engaged stakeholders through structured discussions and presentations to not only communicate their responsibilities but also to demonstrate how IA will help them deliver on those responsibilities.

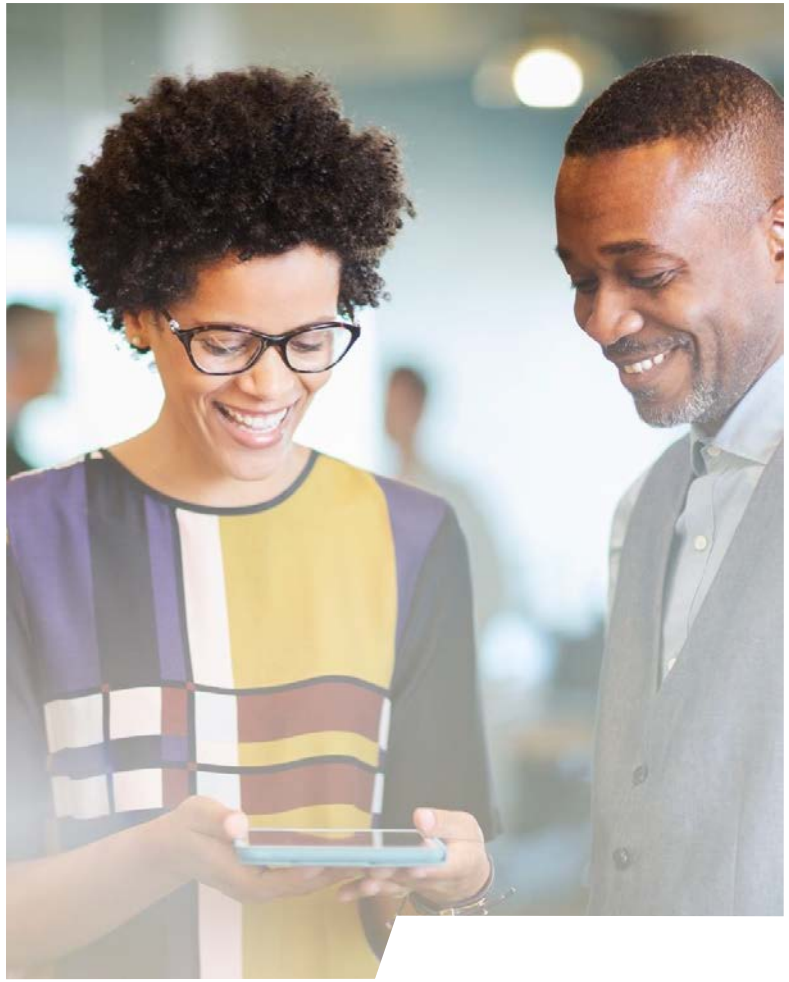
The most common challenge remains striking the right balance on the level of documentation required to evidence conformance; too much can create bureaucracy, but too little risks leaving gaps when assessed through an EQA.

02

IA Strategy (GIAS Principle 9) - emphasises the importance of developing and implementing an IA Strategy that supports the organisation's strategic goals and meets stakeholder expectations.

We still observe differences in how strategies are reviewed and approved. According to the Standards, strategies should undergo regular review and be discussed with the Board and Senior Management. However, many strategies remain as static "on a page" documents, disconnected from enterprise priorities and lacking clear delivery plans.

Leading functions demonstrate strong 'golden thread' linking the IA strategy to organisational goals, convert this into KPIs, and review the strategy with the Board at least once a year to maintain its relevance.



Common challenges and early experience with the new Standards (continued)

03

Topical Requirements (GIAS) - specific requirements set out by the IIA to be used when providing assurance on a specified risk area.

The introduction of Topical Requirements under GIAS is a major step to driving improvements in consistency and quality across the profession. The first requirement on cybersecurity has already been released, with others including third-party, organisational resilience, and organisational behavior expected to publish later this year. The Code also reinforces this agenda, with Principle 8b requiring IA to conduct risk-based reviews of culture.

Although the first topical requirement does not take effect until February 2026, many functions are already reviewing and some adopting the guidance. The newly issued IIA's Topical Requirements Application Guidance is important, as it makes clear that not every requirement will apply in every engagement, but IA must document its rationale for inclusion or exclusion.

Selected functions are benchmarking against frameworks such as the U.S. National Institute of Standards and Technology (NIST)'s Cybersecurity Framework (CSF), piloting reviews, and building evidence trails. Some CAEs remain cautious, concerned the requirements may be too prescriptive. The real opportunity is to apply proportionality while meeting a global baseline. Those who adopt early, document decisions, and engage stakeholders will be best placed to demonstrate maturity when the requirements become effective.

04

Insights from IA, Reporting and Conclusion Statements (GIAS Domain I, Standards 11.3, 14.5 and 15.1; Code Principle 11) - focuses on providing overall conclusion on the effectiveness of governance, risk management and control ('GRC').

While reporting formats continue to evolve, many IA functions still fall short of the requirements to provide an annual overall conclusion. Beyond compliance, there is also a growing expectation for IA to provide insights and foresights. The Standards (Domain I: Demonstrating Value Beyond Compliance) and the Code both emphasise the need for IA to enhance organisational value by helping stakeholders anticipate emerging risks.

We have seen leading functions excel by performing read-across analysis, for example, drawing out patterns by product lines, revenue streams, or regional performance to highlight systemic issues and forward-looking implications. This ability to connect the dots and provide an enterprise-level perspective is increasingly what distinguishes IA functions that are simply compliant from those regarded as truly value-adding.

Common challenges and early experience with the new Standards (continued)

05

Quality Assurance and Improvement Programme ('QAIP') (Standards 17.1–17.3; Code Principle 13) - not a new requirement however this remains one of the most common areas of weakness.

We continue to see undocumented QAIPs, internal quality assessments not performed annually, results not shared with the Board or senior management, and action plans that are not tracked. The Standards are clear: a QAIP must include an annual internal quality assessment, with results communicated to the Board and senior management, and improvement actions incorporated and progress monitored. Yet in practice, QAIPs often remain underdeveloped, inconsistently applied, or entirely absent.

High-performing functions treat QAIP as a catalyst for continuous improvement rather than a compliance exercise. Leading teams escalate findings to the Audit Committee, track actions openly, and link QA outputs directly to capability development. We have also seen functions where QA coverage extends beyond audit delivery into a wider "QA universe", encompassing annual planning and risk assessment, stakeholder engagement, reporting and strategic initiatives. This broader approach ensures QA insights drive continuous improvement rather than being confined to post-audit reviews. By contrast, common pitfalls include QA that focuses too narrowly on audit execution, or varied maturity levels where no internal assessments are performed and no overall view of conformance is presented to the Board.

06

IA Performance Objectives and Effectiveness (Standards 9.2 and 16.1; Code Principle 12) - require the CAE to operate a performance measurement programme, with the Board approving Internal Audit's objectives annually.

The requirement for IA to set objectives is not new, but it is now made more explicit under the Standards and Code. CAEs are required to establish a performance measurement programme for the function, with the Board being responsible for approving IA's objectives annually and for assessing the function's effectiveness at least once a year. The Code reinforces this by requiring the Board and senior management to provide input into shaping IA's performance objectives, with final approval by the Board.

We have seen leading functions align KPIs with the IA mandate and the organisation's wider strategy, securing endorsement from both senior management and the Board. They are also adopting digital tools and data analytics to track KPI data dynamically through dashboards, providing real-time insights that support improvement programmes and enhance stakeholder reporting. This approach transforms performance management from a compliance exercise into a strategic enabler of functional growth and maturity.

Common challenges and early experience with the new Standards (continued)

07

Coordinated Assurance and Reliance (Standards 10.2; Code Principle 5) - place emphasis on Internal Audit coordinating with other assurance providers to avoid duplication, identify gaps, and present a holistic view of risks.

In practice, we continue to see challenges where many organisations lack a structured framework for coordinated assurance. This is often the result of varied levels of maturity across the three lines of defence, with risk and issue taxonomies that are misaligned, inconsistent documentation standards, and fragmented reporting to the Board. The outcome is predictable: inefficiencies, duplication of effort, and blind spots in assurance coverage. In selected cases, IA functions (often under an agreed mandate with their Board Audit Committee) adopt a firm position of placing no reliance on the work of other assurance providers.

By contrast, a number of mature and leading functions are embracing a more integrated approach. They are developing coordinated assurance maps and establishing governance forums with second-line functions to promote alignment. Common risk and control taxonomies are agreed, supported by integrated GRC systems. Roles and responsibilities are clear, and the extent to which reliance can be placed on other assurance providers is formally defined.

Proactive collaboration across the lines of defence enables a coordinated assurance framework and plan for the Audit Committee, giving clearer oversight of coverage and highlighting assurance gaps. By reducing duplication and coordinating requirements across an increasingly demanding regulatory landscape, organisations can ensure that assurance activity remains proportionate, efficient and focused on the risks that matter most.

Linkage to the UK Corporate Governance Code Provision 29

The revised UK Corporate Governance Code (2024) applies from 1 January 2025, with Provision 29 effective for years beginning on or after 1 January 2026. Provision 29 heightens Board accountability by requiring premium-listed companies to provide an annual declaration on the effectiveness of their risk management and internal control framework, supported by a clear explanation. This represents a step change: moving beyond compliance to a requirement for Boards to demonstrate confidence in both the design and operation of their framework.

Boards and Audit Committees will increasingly look to IA for independent assurance, working in close coordination with the second line, to support a robust and defensible declaration. In many organisations, IA is already acting as a programme assurance partner for readiness. In others, particularly where the second line of defence is strong and well established, the emphasis may be on IA linking in and aligning assurance activity rather than leading it. Over time, IA may play a more active role as an integrator of assurance across the three lines of defence, though the balance of responsibilities between the second and third lines varies by organisation.

The combined effect of the GIAS and Provision 29 is encouraging organisations to:

- Align assurance planning across the second and third lines to reduce overlap and highlight gaps;
- Share data and insights more systematically to strengthen the overall risk narrative; and
- Be transparent about reliance, with IA clearly stating where other assurance work has been considered.

This does not diminish IA's independence. Rather, it strengthens its role as the third line of defence, ensuring the Board sees a coherent, evidence-based picture of assurance activity and control effectiveness, which is essential for delivering a credible Provision 29 declaration.

Click here to read more PwC's Spotlight on Material Controls

Common challenges and early experience with the new Standards (continued)

08

Culture audits: scope, delivery and evolving practice (Code Principle 8b) - approaches to culture audits still vary widely across organisations.

The Code explicitly requires IA to undertake risk-based reviews of organisational culture, including the tone set by leadership and the alignment of behaviours with stated values and ethics. To conform, functions must ensure delivery is evidence-based and objective, drawing on multiple data sources such as employee surveys, whistleblowing data, HR metrics, thematic reviews, and stakeholder interviews. Without triangulation across these inputs, conclusions risk being conclusions risk being perceived as anecdotal or lacking rigour..

Some IA functions incorporate management awareness ratings in their reports; others break culture into specific themes such as leadership behaviours, decision-making, or accountability; while some embed cultural assessments into broader audits such as Health & Safety, Conduct, or HR.

Leading functions are developing structured methodologies for cultural assurance that combine targeted deep dives with broader organisation-wide assessments. In some cases, culture or behavioural specialists are engaged to design and deliver these reviews, adding expertise in assessing values and behaviours. Increasingly, functions are also leveraging data analytics and sentiment analysis tools to identify patterns and detect emerging cultural risks.

Crucially, culture audits should not be treated as one-off exercises but embedded in the audit universe as recurring themes. This provides Boards and Audit Committees with clearer visibility of cultural strengths and weaknesses, as well as early warning indicators of behavioural misalignment before issues escalate into regulatory, reputational, or operational challenges.

Preparing for EQAs under the new Standards

Overview

Under the 2025 *Global Internal Audit Standards*, expectations around External Quality Assessments (EQAs) have been significantly strengthened. While the minimum of five-year assessment cycle still applies, the new Standards bring greater rigour, clearer accountability, and stronger Board involvement.

A key change is the requirement for the Chief Audit Executive (CAE) to actively engage the Board in planning the EQA, including the method, timing, and scope. This takes assessments beyond a box-ticking exercise and instead requires structured, strategic discussion with relevant stakeholders, including senior management.

The Standards now also specify that the results of a full EQA must go directly to the Board, reinforcing accountability at the highest level. Another important change is the expectation around assessor qualifications: at least one member of the assessment team must hold an active Certified Internal Auditor (CIA) designation. This should be explicitly addressed when confirming the scope and appointment of the external assessor.

The IIA's Quality Assessment Manual and the Four-Point Quality Rating Scale

The *Quality Assessment Manual*, updated in late 2024, sets out the IIA's expectations for evaluating IA functions. The most visible change is the introduction of a new four-point quality rating scale, replacing the former binary approach. The highest rating of Fully Conforms is now reserved for functions that not only meet the Standards but also demonstrate maturity, impact, and consistent performance.

Our point of view

This new model has sparked active debate. For example, what really differentiates "Fully Conforms" from "Generally Conforms"? Our view is that to achieve "Fully Conforms," a function must provide sufficient and appropriate evidence that each principle and Standard is fully met, in both design and intent, and that practices are consistently in place and working as expected. "Generally Conforms" recognises some differences against the Standards, so long as the intent is still achieved. In practice, most functions will find "Fully Conforms" difficult to achieve in the early years, and group functions may face additional complexity when balancing local assessments against the group-level outcome.

It is important to emphasise that **not achieving "Fully Conforms" does not mean a function is** ineffective. Effectiveness should be measured by the extent of consistency, reliability, and maturity demonstrated over time. Many Boards recognise the need to weigh the investment required to achieve full conformance against other priorities. For most IA functions, "Generally Conforms" will remain a credible and respected outcome, provided there is clear evidence that the intent of the Standards is achieved and that the function demonstrates a commitment to continuous improvement.

Preparing for EQAs under the new Standards (continued)

What have we learned so far, and what to expect next?

With only one year of implementation, adoption of the new Standards is still in its early stages, and the bar for conformance will continue to evolve as the profession gains experience. So far, we have observed three key takeaways:

- Full conformance is possible but demanding, requiring robust evidence and consistency across all Standards.
- Professional judgement is critical, and needs to be documented clearly and transparently. Decision logic should always be recorded, and teams should be ready to explain and evidence, where applicable.
- Maturity matters, even if it is not rated, as it shapes the narrative of an EQA and demonstrates Internal Audit's impact beyond compliance. Functions can demonstrate maturity through evidence of continuous improvement under their QAIP, stakeholder engagement, innovation, adoption of technology, and adaptability to business change.

Looking ahead, we expect greater clarity to emerge from the first wave of EQAs under the new Standards, particularly on how assessors distinguish between "Fully Conforms" and "Generally Conforms," and how maturity narratives are received by Boards. For CAEs, the lesson is clear: treat EQAs not just as a compliance milestone, but as a strategic opportunity to demonstrate maturity, reinforce credibility, and demonstrate how IA is delivering value to the organisation.

Preparing for your next EQA

Based on our experience, IA functions preparing for an EQA should focus on the following:

- Maintain governance oversight: Engage the Board and senior management throughout to ensure alignment, visible oversight, and conformance with the Standards.
- Define scope and requirements early: Work with the Audit Committee Chair and stakeholders to agree the purpose, scope, and timing of the EQA, including regional / jurisdictional coverage, treatment of in-progress transformation or new tools, and consideration of IIA topical requirements.
- Complete a self-assessment: Use the IIA's Quality Assessment Manual to benchmark against the Standards, feed improvement actions into your QAIP, and communicate progress transparently to the Board.
- Collate key documentation: Ensure strategy, QAIP, audit plans, resourcing plans and budget, methodologies, and other core materials are ready for review.
- Plan engagement activities: Prepare for interviews with stakeholders (both IA and the business), document self-identified issues, and provide evidence of how they are being addressed.
- Consider a maturity assessment: While optional, maturity and peer benchmarking can add valuable insight and help shape the EQA narrative.

AI in Internal Audit

Overview

IA functions are under increasing pressure to deliver broader assurance, sharper insights, and greater responsiveness to change. Traditional approaches built around cyclical reviews and sample testing are often too slow and narrow to match the pace at which risks now emerge. To remain relevant and impactful, IA must evolve its methodologies and toolset, expanding use of technology to enhance both efficiency and coverage.

AI in particular offers a step-change. Unlike earlier generations of automation, AI can read, reason, and generate outputs across vast datasets, enabling IA to expand its reach, accelerate reviews, and provide more tailored insights. This opens the door to more continuous, risk-weighted assurance, moving beyond retrospective testing to reflect how organisations operate today.

If used responsibly and strategically, AI can also strengthen IA's advisory role. By surfacing emerging risks such as cyber resilience and the governance of AI itself, functions can provide the Boards and Audit Committees with forward-looking insight while maintaining independence and rigour. This section explores how AI can be applied across the IA lifecycle and the practical steps needed to successfully embed AI into IA working practices.

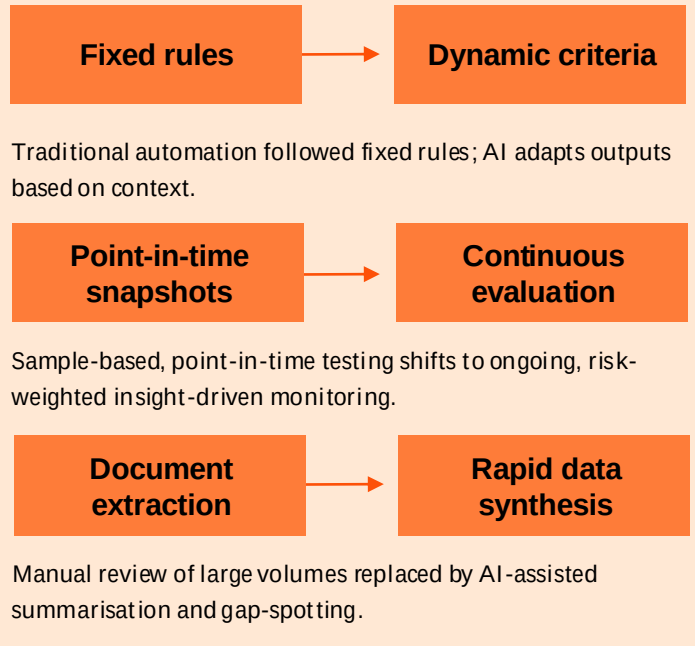
Assurance-in-the-loop: how AI is reshaping IA

AI reshapes assurance in two ways:

- First, IA must *assure with AI,* applying AI capabilities across planning, fieldwork and reporting to widen coverage and shorten audit cycles.
- Second, IA must *assure AI itself,* treating AI systems as a source of enterprise risk, applying proportionate, repeatable checks to validate how they behave and where accountability lies.

The result is a shift from periodic, sample-based testing to what we call **"assurance-in-the-loop"** routine: a risk-weighted evaluation that uses information the business already holds, including policies, activity logs, outcomes and incidents to provide earlier, clearer insight into how AI-enabled processes behave over time.

If done well, this expands IA's reach and the insights it can provide, raising the bar on coverage and timeliness, and moving from a conventional approach to an AI-driven one. At the same time, it reinforces IA's commitment to its core principles: evidence, independence, and professional judgement. The diagram on the right illustrates how an AI-driven approach could transform a conventional IA approach.



Tangible benefits to IA:

Increased coverage: Full populations tested, more scenarios examined, with stronger analysis, and linkage across control design and testing outcome.

Faster cycles: Shorter time from scoping to findings in document-heavy audits (e.g. compliance, governance)

Improved quality with consistency: First drafts that are consistent, well-sourced and tailored to each audience, minimising rework.

Earlier detection of anomalies: Detects shifts in behaviour or risks sooner, helping redirect audit effort to priority areas.

The next page features a case study showing how AI is transforming IA and delivering these benefits.

AI in Internal Audit (continued)

Case Study: From weeks to minutes – How AI reinvented reporting and follow-up

A global consumer goods group piloted generative AI in its Internal Audit function to cut reporting time without compromising quality. Within the first cycle, drafting moved from weeks to days and follow-up shifted from reactive to predictive, while maintaining full traceability and human sign-off. The pilot established a repeatable approach that now supports assurance-in-the-loop across reporting and follow-up.

The challenge

Audit teams were spending up to three weeks drafting reports after fieldwork. Walkthrough notes, meeting transcripts and evidence logs accumulated, and turning them into a clear narrative was slow and error-prone. Follow-up was largely reactive: overdue actions surfaced at quarter-end, leaving little time for remediation before Audit Committee meetings.

The AI-powered approach

- **Theme extraction at scale.** A secure, generative-AI workbench integrated with the audit platform processed more than 50 interview and walkthrough transcripts, clustering recurring issues such as 'access hygiene' and 'supplier Service Level Agreement (SLA) gaps'. These themes informed the executive summary and the Audit Committee narrative.
- **Two-minute drafts.** After fieldwork, auditors uploaded structured evidence and key observations. The tool produced a first draft in about two minutes, with well-articulated context, risk statements and suggested proportionate recommendations: each linked to the underlying evidence. A human reviewer validated the draft prior to issuance.
- **Predictive follow-up.** A machine-learning model analysed existing metadata (issue owner, complexity, IT dependencies) to flag actions likely to miss deadlines. At-risk items appeared on a dashboard, enabling earlier escalation and re-planning.

The impact

- Report cycle time reduced from 15 days to 3 days.
- Audit Committee packs added a concise 'risk of slippage' heatmap, improving oversight.
- Auditors reported higher engagement, spending more time on root-cause analysis and stakeholder discussion, and less on formatting.

AI in Internal Audit (continued)

Given the breadth of the IA lifecycle, AI can be introduced to enhance consistency, speed, and coverage, while ensuring outputs remain fully traceable and reviewable. To achieve this responsibly, we group AI applications into an "AI Capability Stack": a phased approach that enables auditors to adopt AI progressively and effectively. The stack has three layers of capability: Assistants, Analysts, and Agents. The following section explains each layer and provides use cases to illustrate how AI can reinvent conventional IA approaches.

(i) Assistants: *help auditors work faster by securely searching approved information and drafting materials with clear references.*

Use cases:

- Policy recall: Retrieve exact passages from approved regulatory/policy libraries in response to queries (e.g. "What are GDPR's requirements on data retention?").
- Automated drafting: Generate first drafts of scoping documents or audit reports from historic templates.
- Meeting prep: Compile summaries of prior findings, management actions, and relevant standards before walkthroughs.
- Evidence collation: Convert interview notes into structured first drafts of control descriptions or process narratives.

(ii) Analysts: *support structured analysis by guiding auditors through scoping, testing, and reporting in line with methodology, making work more consistent and reliable.*

Use cases:

- Scoping & risk assessment: Prompt auditors with plain-language questions (e.g. *"What decisions does this tool influence? What happens if it fails?"*) and structure responses into a risk framework.
- Testing workflows: Provide structured test scripts for areas like payroll processing, supplier onboarding, or IT change management.
- Issue trend analysis: Identify recurring issues or weak themes by analysing historic audit findings (e.g. procurement delays, repeated HR compliance gaps).
- Consistency checks: Benchmark sampled files (e.g. employee expenses, supplier contracts) against thresholds or industry practice for proportionality.

(iii) Agents: *carry out standard tasks or tests on approved data automatically, recording every step so results can be repeated and reviewed with confidence.*

Use cases:

- Data accuracy testing: Run reconciliations of HR, finance, or inventory records against source systems, flagging missing fields or inconsistencies.
- Transaction monitoring: Replay test scenarios for procurement approvals or health & safety incident logging, checking whether thresholds, escalations and audit trails match policy.
- Access control checks: Continuously test joiner–mover–leaver data against HR records to detect access exceptions.
- Model validation: Run scripts against AI/ML tools in use (e.g. credit scoring, demand forecasting), capturing inputs/outputs to create a repeatable evidence pack.
- Third-party assurance: Automate periodic checks on outsourced service provider data (e.g. payroll, logistics, IT support), flag whether reconciliations were complete and within SLA.

AI in Internal Audit (continued)

Bringing it all together

Having considered how AI can support auditors responsibly and where capabilities can be embedded, it is equally important to recognise that people, processes, technology, and culture must evolve together. To manage this effectively, IA should assess maturity on two dimensions: (i) the organisation's maturity in deploying and governing AI, and (ii) IA's maturity in assuring it. These will not always progress in parallel. An organisation may be advanced in AI adoption while IA is still building baseline literacy, or IA may mature its assurance methods ahead of enterprise deployment. Balancing both dimensions is critical to setting the right pace, skills, and safeguards.

The following brings this to life through the four areas of consideration: people, process, technology, and culture, together with an illustrative roadmap for AI adoption, which outline how IA can build capability progressively while maintaining trust and independence.

People: Building skills and defining roles

- All auditors should build baseline literacy in AI: what it can and cannot do, and how to interpret AI-related evidence.
- Selected staff need deeper expertise in evaluation design, data fluency and model risk.
- New roles may emerge, such as Assurance Engineers (designing test packs), IA AI Product Owners (governing audit tools), and AI Evaluation Leads (defining thresholds and quality checks).

Technology: Phased and responsible adoption

- Start with Assistants (secure search and drafting over approved sources).
- Progress to Analysts (guided workflows for scoping, testing and reporting).
- Mature into Agents (controlled automations that run standard test packs with repeatable results).
- The above phased path allows IA to learn quickly, prove value, then automate safely.

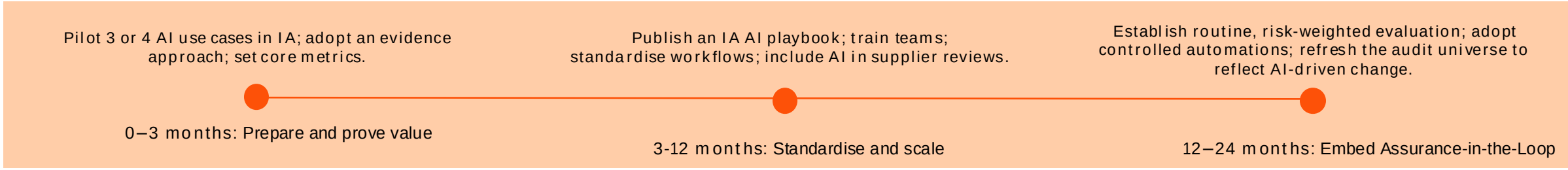
Process: Methods that safeguard quality

- Standardise scoping prompts when AI is in scope: purpose, data used, decisions influenced, expected controls, monitoring.
- Update methodology and workpapers to include an 'AI Evidence' page for any AI-assisted step.
- Build proportionate retention rules and link AI expectations into supplier management.

Culture: Putting independence and judgement first

- Human sign-off remains essential: AI supports coverage and speed, not final decision-making.
- Apply a learning loop: use review notes and rework to refine prompts, sources and test packs.
- Safeguard confidentiality by keeping sensitive data within approved environments.

Illustrative roadmap for adopting AI in IA:



Glossary

Glossary of acronyms and abbreviations

AI/ML/DL	Artificial Intelligence/Machine Learning/Deep Learning
APP	Authorised Push Payment
AWM	Asset and Wealth Management
BAU	Business As Usual
BoE	Bank of England
CASS	Client Asset Sourcebook
CP	Consultation Paper
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CFTC	Commodity Futures Trading Commission
CSDDD	Corporate Sustainability Due Diligence Directive
CSP	Cloud Service Provider
CSRD	Corporate Sustainability Reporting Directive
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
ECCTA	Economic Crime and Corporate Transparency Act
EMR	Electronic Money Regulations
EMIR	European Market Infrastructure Regulation
ESAs	European Supervisory Authorities
ESRS	European Sustainability Reporting Standards
ESG	Environment, Social and Corporate Governance
EU	European Union

Glossary of acronyms and abbreviations (continued)

FCA	Financial Conduct Authority
FRC	Financial Reporting Council
FRTB	Fundamental Review of the Trading Book
FS	Financial Services
GDP	Gross Domestic Product
GI	General Insurance
HM	His Majesty
HMT	His Majesty's Treasury
IAM	Identity and Access Management
IBS	Integrated Business Services
IFPR	Investment Firms Prudential Regime
IFRS	International Financial Reporting Standards
IM(A)	Internal Model (Approach)
IRB(A)	Internal Ratings Based (Approach)
KPIs	Key Performance Indicators
LDI	Liability Driven Investment
MARA	Market Abuse Risk Assessment
MiFID	Markets in Financial Instruments Directive
MiFIR	Markets in Financial Instruments Regulation
ML	Machine Learning
MRM	Model Risk Management
NATO	North Atlantic Treaty Organisation
NIST	National Institute of Standards and Technology, United States
OFTR	Own Funds Threshold Requirements
PAM	Privileged Access Management
PAYE	Pay As You Earn

Glossary of acronyms and abbreviations (continued)

PRA	Prudential Regulation Authority
PSD2	Payment Services Directive 2
PSP	Payment Service Provider
PSR	Payment Systems Regulator
PSRs	Payment Services Regulations
SCA	Strong Customer Authentication
SMCR	Senior Managers and Certification Regime
SMF	Senior Management Function
SRS	Sustainability Reporting Standards
TCFD	Taskforce on Climate-related Financial Disclosures
TCR	Transitional Capital Regime
TPRM	Third Party Risk Management
UK	United Kingdom
UN	United Nations
US	United States

Contact us

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:

Laura McSweeney

I&AWM Internal Audit Leader

Director

+44 (0) 7889 643707

laura.mcsweeney@pwc.com

Steve Frizzell

UK Internal Audit Leader

Partner

+44 (0) 7802 659053

steve.j.frizzell@pwc.com

Richa Dwivedi

Internal Audit - Technology

Senior Manager

+ 44 (0) 7841 468113

richa.dwivedi@pwc.com

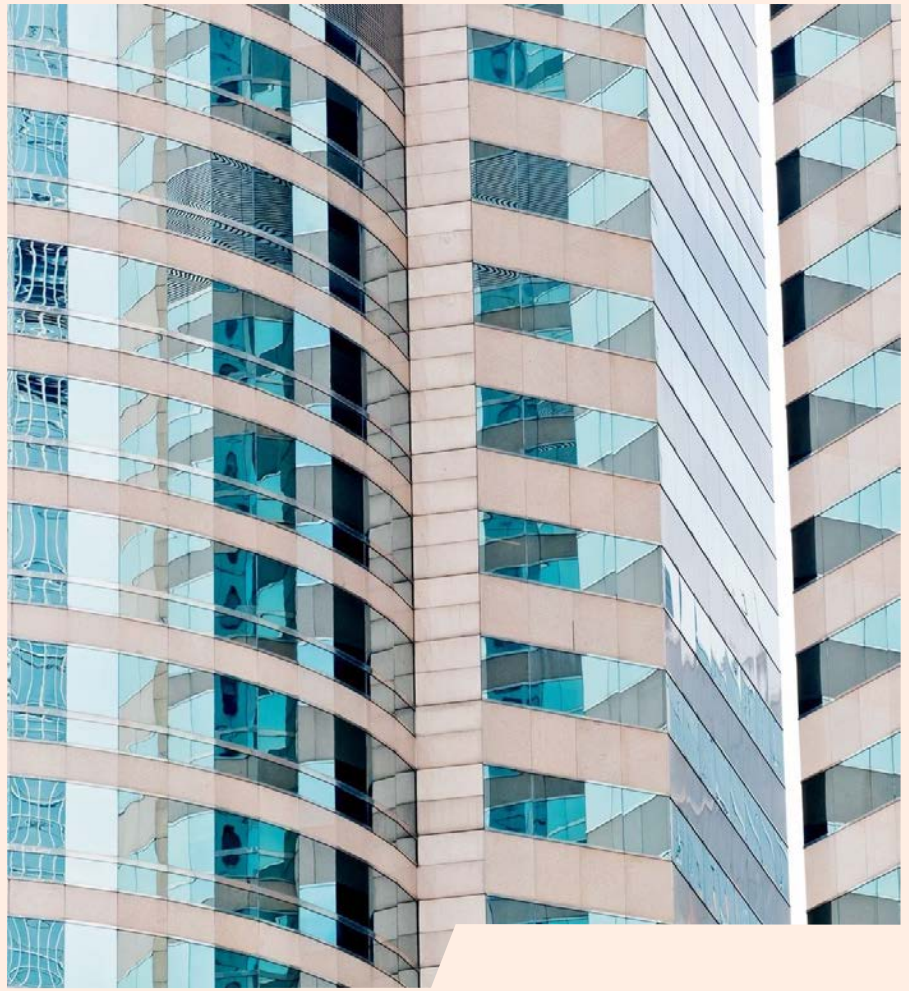
Jia Ying Lim

FS Internal Audit

Senior Manager

+44 (0) 7483 426653

jia.x.lim@pwc.com



Thank you

pwc.com