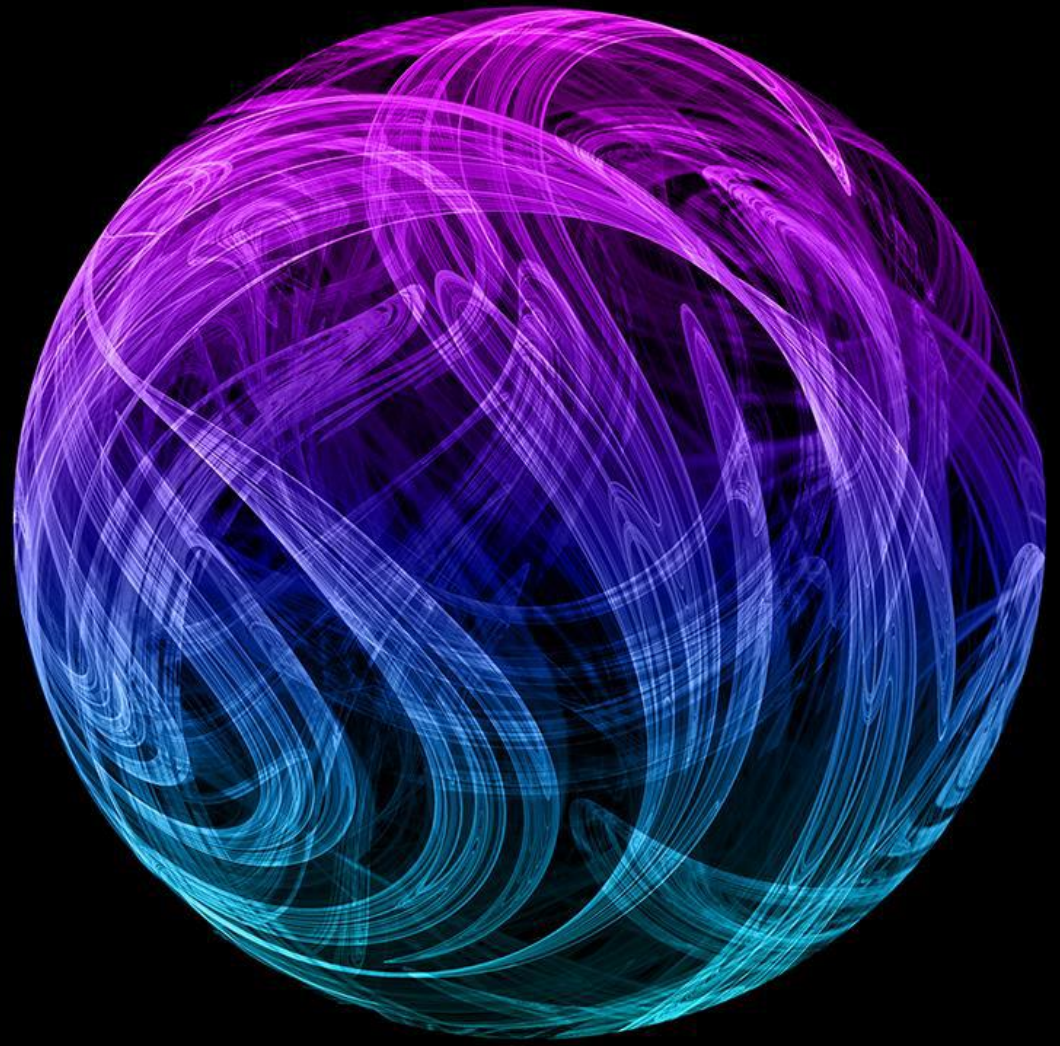
Deloitte.



Financial services

Internal audit planning priorities 2026

Navigate uncertainty: future-proofing financial services

Executive summary

The financial services landscape has been set amid a backdrop of ongoing uncertainty and global disruptions. For financial services organisations, staying resilient in this environment is more important than ever. Three emerging areas are to be considered as firms prepare for the future, both near- and far-term. These include geopolitical risk, GenAI adoption and regulatory simplification.

The nature of geopolitical risk is complex and intertwined with all other risk areas affecting financial services. For internal audit to effectively leverage its unique position, a broad understanding of how potential geopolitical events will impact individual risk profiles with their organisation is key. This holistic view enables internal audit to provide more insightful and strategic guidance in navigating the evolving geopolitical risk landscape.

The growing adoption and normalisation of emerging technologies at all levels of business and society demonstrate how technology is transforming into an environment we inhabit, not just a tool to access. As GenAI becomes further deployed, while the rapidly evolving area of agentic AI materialises, responsible use of technology is paramount to achieve productive growth for the future. What's more, the speed of regulation building around GenAI may drive risk functions to seek more support for technology-related assurance. The increased efficiency gained from integrating Generative AI into internal audit will necessitate an evolving role for the internal audit profession, requiring enhanced strategic evaluation skills. For instance, if real-time reporting is rolled out in the future, the role of the internal audit personnel, department and skillset will need to be prepared for a transformed operation.

Meanwhile, the changing regulatory landscape is driving an overhaul in both organisations and populations globally. Differences in regulatory progress across geographies have created divergent environments for growth and global competitiveness. The interest in deregulation in some geographies could see a shift in how much businesses take on risk and therefore impacts the internal audit professionals' role in evaluating how much an organisation is moving up that risk curve.

For internal audit professionals, emerging regulation could suggest new specialisms in the internal audit discipline as workflows and reporting mechanisms could be affected by regulation and/or deregulation.

Aaron Oxborough
Partner
E: aoxborough@deloitte.co.uk

Matt Cheetham
Partner
E: mcheetham@deloitte.co.uk

Russell Davis
Partner
E: rdavis@deloitte.co.uk

Marc McNulty
Partner
E: marmcnulty@deloitte.co.uk

Yannis Petras
Partner
E: ypetras@deloitte.co.uk

Mahmood Zaman
Director
E: mazaman@deloitte.co.uk

Financial services planning priorities topics overview

Emerging risks	Geopolitical risk and resilience	Responsible adoption of GenAI	Regulatory simplification

Payments and financial crime	Prudential and credit risk	Governance	Environmental, social and governance	Conduct risk	Digital risk and change	Internal audit innovation and transformation	Sector deep dive
Payments regulatory developments	Model risk management	Governance regime	Climate and sustainability risk management	Mortgage rule simplification	Change and transformation	GenAI across IA lifecycle	Global markets
Safeguarding	Credit risk	Risk culture	Sustainability reporting	Motor finance and Buy Now Pay Later (BNPL)	Operational resilience	Data analytics	Pensions
Digital assets	Prudential risk	Integrated assurance		General insurance and premium finance	Third party risk management	High performing internal audit function	Investment management
Fraud	Recovery resolution and solvent exit	Remuneration		Price and value outcomes	Cyber	Standards and QA hotspots	
Financial crime	ICARA				Data governance	Lessons from the field	
					Cloud		

- Cross sector
- Banking and capital markets
- Insurance
- Investment and wealth management

Sections

Click on each section to navigate through the report and use the home button on the right to return to this page.

01

Cross sector and emerging risks

02

Banking and capital markets

03

Insurance

04

Investment and wealth management

Lessons from the field

Key contacts

Cross sector and emerging risks

Emerging risks

Geopolitical risk

Geopolitical risk is paramount in today's volatile global environment. 2025 has delivered many material and unpredictable developments in the world's political and economic landscape. Financial services firms must proactively respond to disruption and external shocks, building resilience by identifying and assessing these risks as part of broader risk management and resilience frameworks. This includes considering the interconnected nature of geopolitical risks and their potential systemic impact.

Internal audit can play a vital role by providing a valuable independent assessment of firms' geopolitical risk management, both at the firmwide level and by evaluating sensitivity to and mitigation of firm-specific risks.

Unlocking internal audit's potential: A strategic lens on geopolitical resilience

- Internal audit is increasingly expected to contribute to the development of a firm's strategy and resilience. With its independence, broad reach and unrestricted access, internal audit is uniquely positioned to provide the board, senior management, and regulators with critical assessments of a firm's geopolitical resilience.

The geopolitical jigsaw: Connecting the dots for enhanced risk management

- Geopolitical risk is not new, but its impact is intensifying. The interconnected nature of geopolitical risk demands a more focused and proactive approach from internal audit.
- The European Banking Authority (EBA) identifies geopolitical risk as a significant concern for the EU/EEA banking sector. The EBA highlights the need for banks to incorporate geopolitical risk into their business strategies and risk management practices.
- Geopolitical risks are increasingly acting as drivers of traditional and emerging risks (it has been featured in over 50% of topics in this publication). Both global and domestic firms face direct and indirect impacts, including:
  - **Financial risks:** Increased credit risk due to deteriorating asset quality, heightened market volatility impacting liquidity and funding, and tariffs disrupting supply chains and tax strategies. Insurers offering political risk, cyber or business interruption insurance face the risk of increasing claims against those policies.
  - **Non-financial risks:** Strategic shifts requiring rapid market exits, operational disruptions from supply chain vulnerabilities and cyberattacks, reputational damage from operating in volatile regions and changing landscape around trade restrictions and sanction compliance regime.

Emerging risks

Geopolitical risk

This interconnectedness raises critical questions for internal audit functions. How can internal audit functions effectively assess and mitigate these interconnected risks?

1. **How can internal audit stay ahead of the curve?**
   - **Maintaining awareness** of geopolitical events impacting the business requires a multi-faceted approach. There's no single definitive source; instead, a combination of news sources, thought leadership, expert networks, and collaboration with economics, compliance, and risk functions is essential for staying informed about evolving market dynamics.
2. **Dynamic risk assessment: adapting internal audit to the pace of change:**
   - Developing a robust strategy to tackle geopolitical risk requires a **shift in mindset**, moving from static planning to dynamic risk assessment. This agility is crucial, as geopolitical risks can emerge and escalate far faster than traditional audit cycles allow.
   - Internal audit's role is not to predict the future, but to assess how well governance, risk management and controls are designed and operating to mitigate the potential impact of geopolitical risks - **a forward-looking lens**, anticipating the potential impact of geopolitical events on various risks, is essential in today's volatile environment.
   - While existing audit plans may adequately cover high-risk areas, the impact of geopolitical events on lower-risk and less frequently audited areas demands increased attention. Internal audit must also consider how **these events can reshape the risk landscape**, for example, rapidly rising inflation driven by geopolitical tensions can exacerbate interest rate risk.
   - **Integrating geopolitical risk assessment** into relevant audit planning discussions with stakeholders is paramount. Breaking down silos and fostering collaboration within the internal audit function (e.g. to address business, regulatory and technology risk) is no longer a best practice—**it is a necessity**. This collaborative approach enables a more comprehensive understanding of the evolving geopolitical risk landscape.
3. **Collaboration across the three lines of defence:**
   - Clear communication channels and defined ownership are essential for **sharing critical information** about geopolitical risks and coordinating responses across the first, second, and third lines of defence. Regulators may demand swift responses to emerging geopolitical events, requiring firms to have a **dedicated, cross-functional response team** ready to act.
   - A successful integrated assurance approach, uniting the perspectives and expertise of all three lines, is essential for navigating the complexities of geopolitical risk.
4. **Focus on existing coverage of horizon scanning, stress testing and resilience:**
   - Internal audit should assess the firm's current **horizon scanning process**, ensuring timely insights from risk owners across the organisation. As part of audit coverage, it is important to ensure current stress testing and scenario analysis are effective and that underlying models are challenged and refined, using lessons learned from the past events.
   - **Geopolitical risk and business resilience** should be viewed with the same end goal in mind. Operational resilience and broader technology resilience requires firms to understand their key resources and critical third parties required to deliver services to their customers.
5. **Data Driven insights**
   - Timely and accurate risk data is crucial yet often difficult to obtain. Internal audit should understand how existing data challenges might impact relevant risk reporting, and assess data reliability, system adequacy, and reporting processes. These aspects provide the basis of effective MI for informed decision-making in a dynamic geopolitical landscape.
6. **Internal audit's commentary of geopolitical risk:**
   - As part of internal audit's annual conclusion on risk management framework and periodic audit committee reporting, internal audit should highlight the geopolitical factors that affect key areas of the risk management framework.

Emerging risks

Responsible adoption of GenAI

Generative artificial intelligence (GenAI) continues to prove a strong driver for transformation within the financial services industry, unlocking significant value across the front, middle and back-office value chains.

First-to-market, innovation mindsets are now tempered with concern for risk; 30% of respondents to Deloitte's latest State of GenAI in the Enterprise survey indicated difficulty in managing AI risk as a barrier to its adoption, as a reminder of the importance of responsible governance and risk management to supporting safe and scalable adoption. The financial services industry is long familiar with governance structures, and even subject to targeted regulation such as the PRA's SS1/23 for model risk management and BoE's draft FS2/23 for Artificial intelligence and machine learning (ML).

The evolving global regulatory landscape – such as The Colorado AI act of 2024 and the Japanese 2024 AI Governance Framework – increasingly places an importance on and expectation for practices and structures that promote the responsible development and deployment of AI. The EU's AI Act and the UK's approach to AI regulation both emphasise risk management, transparency, and data protection, particularly concerning AI's potential for harm.

Five things you should know about the topic:

- **Increased audit scope and complexity:** GenAI significantly expands the audit universe. Internal audit teams must assess not only the outputs of GenAI systems but also the underlying algorithms, data sources, and model training processes for bias, accuracy, and security vulnerabilities.
- **Data privacy and security risks:** GenAI's reliance on vast datasets raises significant data privacy and security concerns. Internal audit must ensure compliance with data regulations like GDPR, verifying that data handling practices within GenAI applications meet stringent security and privacy standards.
- **Explainability and transparency challenges:** Demand for explainable AI (XAI) is growing; many GenAI models operate as "black boxes," making it difficult to understand their decision-making processes. This lack of transparency poses a challenge for internal audit in assessing the reliability and fairness of GenAI-driven outcomes, particularly in areas like credit scoring or fraud detection.
- **Emerging regulatory landscape:** Regulatory bodies globally are developing frameworks for responsible AI use. In the UK, AI models are governed through the PRA's supervisory statement SS1/23 (see our views on validating GenAI models here). Different regions also have different requirements which operate and legislate at an array of different levels of scrutiny.
- **Impact on internal controls:** GenAI can both strengthen and weaken internal controls. While it can automate control processes, it also introduces new risks related to data integrity, access control, and the potential for malicious use. Internal audit needs to assess the impact of GenAI on existing control frameworks and adapt accordingly.

Five things internal audit should do:

1. **Develop AI audit expertise**

   Internal audit teams need to acquire the necessary skills and knowledge to effectively audit GenAI systems. This includes training on data science techniques, AI model validation methods, and the regulatory landscape surrounding AI.

2. **Assess data privacy and security controls**

   Internal audit should conduct thorough assessments of data privacy and security controls within GenAI applications, ensuring compliance with relevant regulations. This involves reviewing data access controls, encryption methods, and incident response plans. Regular penetration testing and vulnerability assessments are crucial.

3. **Evaluate algorithmic bias and fairness**

   Internal audit must develop methodologies to identify and mitigate algorithmic bias in GenAI models. This requires examining the data used to train the models, assessing the fairness of the model's outputs, and implementing mechanisms to detect and correct biases.

4. **Monitor regulatory developments**

   Internal audit needs to actively monitor the evolving regulatory landscape surrounding AI and ensure that the organisation's use of GenAI remains compliant. This includes staying informed about new regulations, guidance, and best practices.

5. **Understand the business applications and risks of GenAI**

   Internal audit functions should thoroughly understand how the firm uses, or plans to use, GenAI. The business should identify specific use cases, from customer service chatbots to fraud detection, and assess the inherent risks associated with each. This includes risks related to data privacy, algorithmic bias, model explainability, and cybersecurity. Internal audit has a role to play in partnering with the business to identify and understand the rollout of new GenAI capabilities.

Emerging risks

Regulatory simplification

The UK's financial services growth and competitive strategy (FS strategy) has been published alongside many policy documents and consultation papers. The government is seeking to drive a fundamental shift of households' wealth from retail savings to investments, with implications for firms' retail product and funding strategies and advice offerings. The financial services strategy, and a related set of initiatives, are designed to make the UK the "number one destination for financial services businesses by 2035".

Easing the regulatory burden for UK financial services

Several initiatives have been introduced which aim to reduce the compliance burden for firms, including reforms to the Senior Manager & Certification Regime (SMCR); a review of the application of Consumer Duty to wholesale firms; and changes to capital and resolution policies for banks.

Reforms to the Financial Ombudsman Service (FOS), including giving responsibility to the Financial Conduct Authority (FCA) as the final decision-maker and introducing a 10-year limit on claims, are also proposed to improve predictability and reduce market disruption. In the insurance sector, the FCA has published a consultation paper (CP25/12) proposing significant simplifications to regulations, particularly for commercial insurers.

US regulatory shifts

From a global perspective, recent shifts in the US regulatory landscape have significantly impacted several areas, such as mergers and digital assets.

The Federal Deposit Insurance Corporation (FDIC) and Office of the Comptroller of the Currency (OCC) have reversed stricter merger review standards, rescinding previous regulations. The GENIUS Act is now live, establishing a federal regulatory framework for payment stablecoins (PSCs) and acceleration in other jurisdictions are expected in the coming years.

Beyond compliance - a holistic approach to regulatory management

Effective regulatory management is no longer the sole responsibility of specialist functions (compliance, legal, regulatory affairs). A siloed approach to regulatory issues, encompassing their lifecycle, changes in regulations, and remediation, is insufficient for sustained success.

Boards and senior management must adopt a more strategic and holistic approach to regulatory oversight. Compliance, risk, and strategy teams, along with internal audit should form an early view on which elements of the regulations are material to their firm.

Unlocking internal audit's potential: A strategic lens on geopolitical resilience

Three things internal audit should do:

1. **Navigating the shifting landscape:**

To demonstrate its value as a **strategic partner**, internal audit must actively engage with other functions, including the regulatory change team, to anticipate and address the impact of regulatory shifts on the firm. **This collaborative approach** is crucial for effective regulatory management in the current environment.

Internal audit should strategically assess the effectiveness of the regulatory change and transformation programme. Best practices include: (1) integrating the three lines of defence; (2) fostering strong **coordination across jurisdictions and business units**, particularly in larger, geographically diverse organisations; and (3) securing **strong leadership commitment** from the board and senior management to prioritise initiatives and ensure accountability. Furthermore, alignment between the regulatory change programme and any ongoing organisational transformations is crucial.

Internal audit should monitor key risk indicators (KRIs) across regulatory change processes to determine the impact of key regulatory changes on the organisation's operations, **risk profile and appetite**, and control environment.

2. **Dynamic internal audit planning:**

Internal audit should prioritise the revision of the internal audit plan to incorporate the necessary adjustments made to comply with the **simplified regulations**. There is a need to prioritise audits of areas significantly impacted by regulatory changes, specifically when impact is beyond risk appetite and business strategy.

3. **Unlocking internal audit's potential:**

Internal audit can deliver significant value through proactive engagement in regulatory change - **integrated assurance**, achieved through cross-functional collaboration across the three lines of defence, provides real-time insights through change assurance activities. Further, unrestricted access allows internal audit to challenge **compliance culture**, not just identifying weaknesses but also promoting positive behaviours and strengthening organisational resilience.

Internal audit should establish **ongoing monitoring procedures** to track the implementation of the changes and to identify any emerging risks or compliance issues, including highlighting the organisation's preparedness for the changes and more importantly any emerging risks or challenges.

By adopting this proactive approach, internal audit can support the organisation's compliance with simplified regulations, mitigate potential risks, and position itself for continued success in a more competitive environment.

Payments and financial crime

Digital assets

The accelerating growth of digital assets as an asset class presents both significant opportunities and heightened risks. The increased regulatory scrutiny and inherent complexities associated with digital assets demand robust internal audit oversight. We encourage a proactive and risk-based approach to planning and ensuring alignment with the organisation's overall strategic objectives and risk appetite.

Five things you should know about the topic:

- **Evolving digital asset landscape**: The digital asset landscape is evolving, with notable growth being seen in stablecoins, tokenisation of real-world assets (RWA) and decentralised finance (DeFi), alongside the continuous growth of cryptocurrencies.
- **Global regulatory developments**: From a global perspective, the US's approval of Bitcoin and Ethereum ETFs, alongside a more collaborative stance between regulatory agencies and the introduction of targeted legislation (GENIUS Act for stablecoins), signals a move towards an increasingly defined regulatory framework. This shift marks a departure from the previous emphasis on enforcement actions and offers greater clarity for businesses. Across the Asia-Pacific region, jurisdictions like Singapore and Hong Kong are establishing themselves as digital asset hubs by implementing licensing regimes for Virtual Asset Service Providers (VASP) and strengthening consumer protections, including restrictions on retail access and enhanced disclosures.
- **The UK's crypto-asset regulatory framework**: Recent developments, including the Financial Conduct Authority's (FCA) crypto-asset regime and the Bank of England's stablecoin regulations, are introducing new compliance obligations. Draft statutory instruments and FCA Consultation Papers (CP25/14, CP25/15, CP25/16) bring further considerations around client assets sourcebook (CASS), the Prudential Regime, and retail access to crypto-asset exchange-traded notes (cETNs).
- **Data integrity challenges**: Immature frameworks could raise significant data independence concerns, increasing the risk of misreporting, fraud, and regulatory breaches. This can lead to vulnerabilities in areas such as data governance, access control, and transaction processing.
- **Managing conflicts of interest in the digital asset sector**: Failures to manage conflicts of interest in the digital asset sector have led to significant customer losses and market instability. Previous high-profile collapses, such as that of Futures Exchange (FTX), in the sector have underscored the tangible consequences of inadequate conflict management, highlighting the importance of clear governance, segregation of duties, and independent oversight.

Five things internal audit should do:

1. **Regulatory compliance internal audit review**

   Conduct a thorough review of the firm's compliance with the evolving regulatory framework for digital assets. Assess the adequacy of controls designed to mitigate the risk of non-compliance where the firm is already offering products and services to clients.

2. **Data reconciliation and integrity**

   Evaluate the effectiveness of data reconciliation processes, focusing on the independence and integrity of data sources. This evaluation should specifically address reconciliation of key data types, including transaction data wallet balances, custody records, and client account information. Identify and remediate any gaps or weaknesses in existing controls to mitigate the risks of misreporting, fraud, and regulatory breaches, including recommendations for strengthening data governance and control frameworks.

3. **Conflicts of interest assessment**

   Consider performing a comprehensive assessment of the firm's conflicts of interest framework and controls, paying particular attention to the interaction between trading, custody, and other business lines. The goal is to identify and mitigate potential conflicts proactively, ensuring robust and effective mitigation strategies are in place.

4. **Global best practice benchmarking**

   Benchmark the firm's digital asset risk management practices against market standards and regulatory expectations, including horizon scanning to identify emerging best practices and regulatory trends.

5. **Technology and operational resilience**

   Internal audit should conduct a thorough assessment of the firm's technology infrastructure and its ability to support digital asset operations. Identify vulnerabilities and recommend appropriate mitigation strategies to enhance operational resilience against potential disruptions, including an evaluation of the team's technical expertise and a plan to address any gaps.

Payments and financial crime

Fraud

Fraud remains a significant challenge for financial services firms, and its complexity is only expected to increase in 2026. Evolving regulations, technological advancements, and economic uncertainty create new vulnerabilities and opportunities for fraudsters. Internal audit functions must adapt their strategies to effectively identify and help organisations to mitigate these emerging risks.

Five things you should know about the topic:

- **Regulatory scrutiny intensifies:** The UK's regulatory landscape is shifting, with anticipated rulebook changes impacting fraud prevention and detection. Expect a rise in Financial Conduct Authority (FCA) visits and a focus on compliance with evolving requirements.
- **Failure to prevent (FTP) fraud:** With new legislation now in effect, firms must demonstrate robust fraud prevention frameworks, while financial services face a "double threat" from both internal and external fraud, including acts committed by associated persons for the firm's benefit, requiring a holistic approach to address fraud that can either harm or benefit the organisation.
- **Payment systems under pressure:** The Payment Systems Regulator (PSR) is being consolidated with the FCA to reduce “red taping”. The Authorised Push Payment (APP) fraud reimbursement scheme has been live for about a year, giving strong protection to victims of fraud.
- **Global regulatory shifts:** PSD3 in the EU is shifting the liability for fraud from customers to banks and non-bank payment institutions, requiring firms to enhance their fraud detection and prevention capabilities. Similar regulatory changes in Asia, particularly regarding payment infrastructure, will pose challenges, especially for smaller banks and FinTechs.
- **Generative AI (GenAI):** The accessibility of GenAI tools is empowering fraudsters with sophisticated capabilities, including advanced phishing attacks in multiple languages, and large language models (LLMs) are being used to not only conduct impersonation but to also achieve more believable personas in line with relevant product or service offerings provided by financial services institutions. This lowers the barrier to entry to create complex fraud schemes and necessitates new approaches to detection and prevention.

Five things internal audit should do:

1. **Prepare for increased regulatory scrutiny**

   Internal audit should proactively stay informed about upcoming rule changes and perform gap analysis to ensure organisations are prepared to comply with evolving fraud-related regulations. This includes preparing for increased FCA visits and demonstrating readiness for regulatory scrutiny.

2. **Validate FTP framework effectiveness**

   Internal audit should independently assess the design and operational effectiveness of the firm's FTP framework. This involves reviewing ownership, documentation, training programmes, and control effectiveness to ensure alignment with regulatory expectations and industry best practices.

3. **Assess payment systems control design**

   Internal audit should evaluate the design and effectiveness of controls related to payment systems, focusing on compliance with payment rule changes and how it continues to comply with Authorised Push Payment (APP) fraud framework. This includes assessing the adequacy of fraud detection and prevention measures within payment channels.

4. **Evaluate global regulatory compliance**

   Internal audit should assess readiness for global regulatory changes, particularly PSD3 in the EU and similar regulations in Asia, such as the Payments Service Act in Singapore. This includes evaluating the impact of liability shifts and assessing whether adequate controls are in place to address the changing regulatory landscape.

5. **Address GenAI-enabled fraud risks**

   Internal audit should develop a comprehensive understanding of the risks posed by GenAI-enabled fraud, including advanced phishing and other emerging threats. This involves updating fraud risk assessments, exploring new detection techniques, and incorporating GenAI considerations into audit plans.

Payments and financial crime

Financial crime

The continuing evolution of financial crime typologies, coupled with a rapidly changing geopolitical environment, presents significant compliance challenges for organisations to remain resilient. These include responding to the evolving sanctions landscape, responsible integration of generative AI (GenAI) into operations, and leveraging industry lessons in risk assessment frameworks. Internal audit functions should proactively assess these areas to support their organisations in enhancing their effectiveness in combating financial crime, safeguarding organisational integrity, and fostering stakeholder trust. In 2026 and beyond, these priorities will be paramount in maintaining a strong defence against increasingly sophisticated criminal activity.

Given the significant financial crime fines issued recently, strengthening anti-financial crime controls and compliance programmes should be a high priority on the Board's agenda.

Five things you should know about the topic:

- **Robust financial crime enterprise-wide risk assessments (EWRA):** Strong EWRAs are vital for identifying and mitigating evolving threats. Regularly assessing risk identification, measurement, and mitigation strategies is essential, considering emerging risks, guidance, and industry insights.
- **Sanctions compliance:** Agile compliance systems are essential for navigating the evolving sanctions landscape. Effective and adaptable sanctions screening is crucial for mitigating breach risks amidst new designations and regulatory updates.
- **Financial crime target operating model:** A robust operating model is the backbone of effective risk management. Integration of new technologies and data sources into operating models ensure they remain adaptable to the changing regulatory landscape and industry good practice.
- **Responsible GenAI and Machine Learning (ML) integration:** GenAI and ML offer potential but require careful governance. Model validation, bias detection, and explainability are crucial for responsible compliance integration, ensuring human oversight and thoughtful assurance of outputs.
- **Enhanced financial crime monitoring:** Addressing data inconsistencies and fragmentation within internal audit's independent assessments is critical. Data analytics can be utilised to identify patterns and anomalies across disparate sources, improving detection and reporting.

Five things internal audit should do:

1. **Robust risk assessments**

   Critically evaluate the robustness and accuracy of EWRAs, ensuring alignment with regulatory guidance and emerging risks. Focus on the effectiveness of risk mitigation strategies and the integration of risk assessments into decision-making and governance processes.

2. **Deep dive into sanctions compliance**

   Whilst it is important to continue to assess the "basics" in the context of sanctions compliance, internal audit functions should also consider implementing data analytics and scenario-based testing to evaluate the effectiveness of sanctions controls against evolving typologies and evasion techniques.

3. **Holistic assessment of the financial crime target operating model**

   Assess the alignment of the financial crime target operating model with relevant regulatory expectations, industry good practice, the organisation's risk appetite and Consumer Duty principles, recommending opportunities for efficiency such as streamlining processes and leveraging technology where appropriate. This should include evaluating whether the firm's financial crime controls adequately protect vulnerable consumers.

4. **GenAI and ML governance**

   As businesses continue to adopt GenAI and ML, internal audit should consider the robustness of the governance frameworks around such models, with a focus on ethics, data privacy, model validation, and ongoing monitoring.

5. **Data integrity and consistency**

   Focused testing on data quality, data lineage, consistency, and completeness, including assessing whether the organisation is making the most of potential data sharing opportunities across functions.

Prudential and credit risk

Model risk management

Boards and regulators are maintaining their focus on model risk management (MRM) in the face of increasing adoption of models across all business functions. Firms are needing to adapt and expand their risk management framework and capability in order to meet this evolving challenge.

Five things you should know about the topic:

- **Broadening definition of model**: Model risk remains a key area of focus for regulators, who increasingly expect it to be managed as a risk discipline in its own right. The definition of "model" has broadened, encompassing a wider range of tools and techniques, including AI/ML models.
- **Model development:** Model risk is about more than just the model being 'wrong'; it also encompasses risks (and controls) around its development lifecycle, how models are implemented into live systems and their use across the business for decision making.
- **Global regulatory focus:** In the UK in Q3 2025 the Prudential Regulation Authority (PRA) is currently providing bilateral feedback to large firms on the results of their thematic review of compliance with the Supervisory Statement 1/23 'model risk management principles for banks' – this feedback will likely trickle down and impact firms' practices across the industry. For example: it is considered as an expectation to consider under insurers' risk management. Global regulatory scrutiny of model risk is intensifying due to the growing complexity and widespread reliance on model outputs, across in the US (Fed, OCC), EU (ECB) and other regions.
- **Vendor vs. in-house:** Vendor-provided models are emerging as an area of weakness for many firms, where governance and attention have historically been light, but transparency in these models is low and the risks are just as significant as in-house developed models.
- **GenAI acceleration:** Finally, the widespread introduction of Generative AI (GenAI) models is driving a major change in how model risk is perceived and managed. These models have unique features and risk profiles compared to conventional models, which necessitate a joined-up approach across risk and technology functions.

Five things internal audit should do:

1. **MRM for financial and regulatory reporting**

   Assess the effectiveness of model risk controls applied to models used for financial and regulatory reporting. The PRA continues to use the quality of firms' internal model submissions as a yardstick to measure the wider effectiveness of MRM practices. Firms that report under IFRS 9 need to satisfy their audit committees that ECL models are appropriate, including all post model adjustments (PMAs).

2. **MRM framework design**

   Assess the design of the MRM framework, including typical problem areas such as the treatment of deterministic quantitative methods (non-models), management of implementation/usage risks, model inventory review and coverage of vendor models.

3. **Model risk and AI governance**

   Assess the firm's processes for managing risks resulting from the use of GenAI model, including ownership of governance processes and division of responsibility between model risk and other functions e.g. technology, conduct risk, data security.

4. **Independent model validation unit skills and resourcing**

   The depth and frequency of independent model validation reviews is a highly material feature of a proportional, risk-based MRM framework. Internal audit should perform work to assess whether the validation function has the appropriate headcount and skills to discharge its responsibilities.

5. **Financial crime models**

   In many firms, financial crime models have historically been somewhat detached from the governance of risk and finance models, but this is starting to change. Internal audit should assess whether a firm's MRM framework is applied appropriately and consistently across the whole taxonomy of models, including financial crime.

Prudential and credit risk

Recovery and resolution planning (RRP) and solvent exit

Regulators maintain a sharp focus on recovery and resolution planning (RRP). The Bank of England expects demonstrable evidence of firms continuing to embed and enhance their approach, showcasing practical recovery and resolution capabilities under stress.

The key 2025 deliverable is October's "solvent exit planning" for non-systemic deposit takers. In-scope firms must demonstrate compliance with minimum criteria, including "assurance“, by this deadline.

UK insurers face a similar mandate for solvent exit planning under Supervisory Statement SS11/24, with a submission deadline of 30 June 2026. Like the requirements for non-systemic deposit takers, insurers must develop detailed Solvent Exit Execution Plans (SEEPs) if a solvent exit becomes likely.

Six things you should know about the topic:

- **Proving/testing RRP functionality/effectiveness:** Demonstrating the effectiveness and usability of RRP plans in a crisis is crucial. Firms should establish a well-governed testing programme within the first/second line. This demonstrates to management that regulatory requirements are met, and an effective resolution approach is in place.
- **Financial Services Compensation Scheme (FSCS) and single customer view (SCV):** Firms must provide the FSCS with an accurate, timely, regularly reviewed SCV file.
- **Resolvability assessment framework (RAF):** In-scope firms must demonstrate overall resolvability across all eight barriers. The regulator will expect internal audit to review RAF elements at an appropriate frequency, considering size and complexity.
- **Recovery planning:** Firms must continue to embed their recovery plans and demonstrate usability through fire drill testing. Demonstrating 'recovery capacity' effectively has been challenging for some. The guidance in the supervisory statement can be supplemented by the best practice contained in the European Banking Authority (EBA) guidelines on overall recovery capacity.
- **Central Bank Facilities:** The Bank of England expects sterling monetary framework (SMF) participants to maintain eligible collateral for funding shortfalls. Firms should have systems and controls to monitor eligible collateral classes and understand SMF borrowing capacity continuously. Deposit takers should test this regularly to confirm eligibility and operational readiness.
- **Solvent exit analysis:** Non-systemic banks and building societies must complete their solvent exit analysis (SEA) by 1 October 2025. UK Insurers must produce and submit a SEA by 30 June 2026 and prepare a detailed SEEP when a solvent exit becomes likely.

Five things internal audit should do

1. **RRP testing programme assurance**

   Critically evaluate the governance and effectiveness of each firm's RRP testing programme. Focus on demonstrating the usability of recovery and resolution plans under stressed conditions, aligning with regulatory expectations and providing assurance to the board.

2. **RAF compliance and assurance**

   Provide independent assurance over the firm's resolvability by assessing compliance with all eight barriers of the RAF. Focus on the design and effectiveness of controls related to each barrier, identifying any gaps or weaknesses. Ensure your review frequency aligns with regulatory guidance.

3. **Recovery plan effectiveness and capacity**

   Evaluate the practical embedding of recovery plans and the effectiveness of fire drill testing. Pay particular attention to the demonstration of "recovery capacity," leveraging supervisory statement guidance (SS9/17) and EBA best practice to provide valuable insights to management.

4. **Central bank facilities readiness**

   For firms participating in the SMF, assess the adequacy of systems and controls for monitoring eligible collateral and understanding SMF borrowing capacity. Evaluate the robustness of testing procedures for confirming eligibility and operational readiness, ensuring alignment with Bank of England expectations and mitigating potential funding risks.

5. **Solvent exit analysis**

   Supervisory Statement SS2/24 mandates adequate assurance activities for SEA preparations following material changes or at least triennially. The PRA expects evidence of these activities for the first submission in 2025. For UK insurers, provide challenge on the assumptions for reasonableness for solvency and liquidity assessment when assessing SEA for alignment with PRA’s expectations.

Governance

Governance regime

Governance and specifically the desire for clear well-documented accountabilities remain a key focus for regulators . There are a series of changes in the pipeline of which internal audit should be aware, as audit functions will likely be required to assess the implementation plans, design effectiveness and ultimately the operating effectiveness of the various regimes.

In parallel, Boards and executive teams are grappling with significant change programmes, including in many cases meaningful remediation programmes, and may require internal audit's support in providing assurance.

Four things you should know about the topic:

- **What's new with governance under Capital Requirements Directive (CRD) VI?** The EU's sixth CRD VI includes a revised 'fitness and propriety' framework, as well as the requirement to maintain individual statements for key individuals that sets out their roles and a separate document mapping the duties, reporting lines and lines of responsibility of the persons that are part of the governance arrangements.
- **Regulatory joint consultation - reforming the Senior Manager and Certification Regime (SMCR):** HMT, the PRA and FCA have issued consultations on proposed changes to the SMCR. These changes are intended to help reduce administrative burden, lower compliance costs and support the flow of international talent to the UK.
- **Execution risk is a major boardroom concern:** The volume of change that firms are currently experiencing is significant, the drivers vary, but be it business changes, technology advances, regulatory scrutiny or material transactions, the outcome is the same: there is a meaningful amount of execution risk that is a cause for concern in many boardrooms.
- **Refining delegated authorities, finding the right balance:** There is an increasing interest from firms and the regulators in ensuring that there are robust but practical executive governance arrangements in place. One important way in which this is manifesting is a revision of delegated authorities, where companies are seeking to strike the right balance of authority between group executives, business heads subsidiaries and functional roles.

Four things internal audit should do:

1. **Governance under CRD VI**

   Internal audit's focus should be on design effectiveness. Where relevant, internal audit should consider the lessons learned from SMCR, focusing on challenging areas such as technology, operational resilience and data.

2. **SMCR joint paper**

   Internal audit should assess the proposed changes and incorporate into the internal audit plan as required. The proposals include removing the certification regime and allowing the PRA and FCA to develop a more flexible and proportionate regime.

   Internal auditors must recognise that the certification regime is often intertwined with other key processes, including recruitment, performance reviews, and disciplinaries. Therefore, these changes may have wide-ranging interconnections and impacts.

3. **Governance change programmes**

   Ensure that the internal audit plan is adequately covering the current suite of change programmes and that the Board and Audit Committee are comfortable with the scope.

   When assessing the effectiveness of project oversight, internal audit should consider whether there is evidence of senior individuals or forums challenging outcomes as well as monitoring progress; assessing portfolio risk and not just the risk of individual projects; and taking action when there is management stretch, rather than passively accepting the consequences of management stretch.

4. **Executive governance and delegated authorities**

   Internal audit should review the operational effectiveness of existing delegated authorities, to provide assurance that authorities are documented clearly, followed throughout the organisation and escalations or exceptions follow an appropriate process and are supported by adequate MI and documentation.

Governance

Risk culture

Increasingly, financial services regulators across the globe are focusing on the effectiveness of organisations' risk cultures, particularly in the UK, Europe (ECB and CBI) Australia (APRA), the Netherlands (DNB), and Canada (OSFI). This includes stronger enforcement of existing regulations and the introduction of new ones, designed to hold senior management accountable for fostering a strong risk culture. The UK CIIA Code of Practice (effective January 2025) also suggests internal audit should be undertaking reviews of organisational culture. Additionally, the institute of internal auditors (IIA) is looking to finalise topical requirement around organisational behaviour to assess if behaviour is aligned to strategy. Beyond regulatory expectations, organisations that consider how their risk culture can be a source of sustainable competitive advantage are well placed for success and may outperform those with undesirable cultures.

Five things you should know about the topic:

- **Internal audit's increasing role**: Internal audit's role in assessing risk culture is important for ensuring an organisation's long-term health and sustainability. A strong risk culture is not a one-time fix but an ongoing process requiring continuous monitoring and improvement.
- **Digital transformation and the evolving risk landscape**: As our world becomes increasingly digital and technologically advanced, including greater use of AI, this brings many benefits but also increased risk. Organisations need to ensure they have a risk culture that supports more AI adoption (i.e. risk management awareness at all grades, a culture of constructive challenge and clear accountability).
- **Global regulatory perspectives on risk culture**: There is increased regulatory interest in risk culture. The Canadian regulator, OSFI, has raised expectations regarding culture risk management (in November 2024) highlighting that culture can support (or undermine) sound decision-making, prudent risk-taking and effective risk management. The European Central Bank (ECB) recently issued its guide on governance and risk culture, which clarifies their expectations that a healthy risk culture that supports innovation and compliance. The Irish regulator, CBI, highlighted that insurance firms must demonstrate robust consumer protection risk management frameworks, underpinned by a strong challenge culture and effective business-control function engagement, to ensure fair customer outcomes.
- **Effective risk culture framework**: A risk culture framework is essential for anchoring a risk culture review or assessment, as well as designing metrics. One example, the Deloitte risk culture assessment framework, considers both human capital and risk management perspectives to give greater depth of coverage.
- **Cybersecurity and technological advancements:** Organisations are investing heavily in cybersecurity infrastructure and training but are also focusing on fostering a culture of security awareness among employees. This involves promoting reporting mechanisms for security incidents and encouraging a proactive approach to identifying and mitigating potential threats.

Four things internal audit should do:

1. **Expanding your current assessment from risk culture to organisational culture and behaviour**

   Given the IIA's increased emphasis on consistency and the growing regulatory focus on behaviour, internal audit functions must develop a comprehensive audit strategy addressing culture and behaviour. This strategy should ensure behaviours align with strategic objectives, delivering positive outcomes for customers, employees, and society. It should cover audit coverage approach to include various toolkits, such as stand-alone review, thematic review and integrated coverage.

   While some mature internal audit functions benefit from dedicated behavioural risk specialists, all functions should strategically align skills to meet this evolving focus.

2. **Consider diversity, equity and inclusion**

   Growing research suggests a strong correlation between diversity and inclusion and effective risk management. This not only encompasses physical diversity characteristics, but also diversity of thought.

   As recommended by the CIIA Code of Practice, internal audit should incorporate this into their risk culture assessments and broader ESG.

3. **Psychological safety/challenge**

   Regulators continue to focus on the extent to which environments are psychologically safe – that is, where individuals feel free to challenge without fear of retaliation at all levels. Internal audit should consider how this is incorporated into their regular risk culture assessments.

4. **Getting ahead using technology for better culture insights**

   Increasing availability of relevant data (including leveraging data analytics and GenAI) can provide quicker and greater insights into culture which can be used to the internal audit teams to ensure right outcomes are reached.

   Consider a risk culture assessment for AI readiness. A risk culture dashboard can support continuous improvement, which collates relevant metrics and data points, including a qualitative overlay on context (e.g., lessons learned) and historical movements to support the metrics.

Governance

Integrated assurance

Integrated assurance is rapidly becoming a top boardroom priority due to the evolving risk and assurance landscape. The revised UK Corporate Governance Code and the new IIA Standards both call for a stronger, more transparent oversight, streamlined risk management and cohesive assurance activities. Integrated assurance is gaining serious momentum as organisations struggle with rising assurance cost, duplicated efforts and fragmented reporting. These developments signal a shift from siloed assurance activities to a connected assurance model that provides clarity of risk coverage across the three lines of defence, eliminates duplicated efforts, and provides an aggregated view of assurance outcomes for greater value and confidence in decision making.

Five things you should know about the topic:

- **Digitisation is unlocking new potential**: The ongoing digitalisation of business processes, transactions, and relationships, along with the decreasing cost and increasing accessibility of digital technologies, holds tremendous potential for assurance, compliance, and risk management functions.
- **Connected organisations perform better**: Organisations that integrate their approach to assurance, compliance and risk across the three lines will be better able to eliminate redundancies. This will foster synergy between different assurance activities, streamline processes, increase efficiency, and reduce the overall cost of compliance, allowing for better resource allocation, improved performance and productivity, and enhanced profitability.
- **Duplication driving inefficiency**: Siloed assurance activities often lead to inconsistent testing and reporting and gaps in coverage. Integrated assurance enables cross-functional coordination, helping to eliminate duplication and reduce the assurance burden. The 2025 IPPF standards mandate the coordination with other internal and external assurance providers to avoid duplication and add value.
- **Real-time insights and aggregated assurance are the new standard**: Static reporting and retrospective views are being replaced by real-time dashboards and dynamic analytics that aggregate assurance aligned with material risks and control. This alignment and improved time to value empower faster and more informed management decisions.
- **Board and executive need a clear view**: The revised UK Corporate Governance Code, particularly Provision 29, has spurred a renewed focus on integrated assurance. This is driven by the Code's increased emphasis on board accountability for robust internal controls, a focus on material risks, the need for director expertise in challenging management on risk and assurance, and the requirement for transparent reporting on control effectiveness. Integrated assurance directly addresses these demands, providing a more efficient and comprehensive approach to risk management and assurance than siloed methods. Senior leadership can no longer afford blind spots. Integrated assurance gives boards and executives a single, cohesive view of assurance and its outcomes – ensuring they are equipped to fulfil oversight responsibilities confidently and proactively.

Three things internal audit should do:

1. **Ascertain your position and make a case for change**

   Achieving the full benefits of assurance, compliance, and risk management requires a strategic transformation, incorporating automation and integration.

   Charting the right course for the organisation is only the first step; securing buy-in for that direction, particularly from senior leadership, is crucial for successful implementation. This requires a compelling business case, typically demonstrating cost reduction, performance enhancement, and improved business resilience.

2. **Create a roadmap and/or clarify your existing roadmap and assurance framework**
   - Establishing a unified ‘one view’: Aligning with the organisation's key risks, terminology (e.g., risk categories, taxonomy), assessment criteria, Audit Universe design, control frameworks, and compliance requirements, ideally through a single, integrated technology platform (GRC tool).
   - Understanding risk appetite and assurance needs: Clear linkage to organisational risk appetite and the required assurance response for each major risk category, including coverage, depth, frequency, required independence of the assurance provider, etc.
   - Defining assurance roles and responsibilities: Identifying primary assurance providers and secondary users, establishing minimum quality expectations for assurance activities.
   - Developing coordinating governance processes: Contributing to the development of governance processes, such as an "assurance traffic control" mechanism, to coordinate assurance activities and minimise duplication.
   - Integrated reporting: Develop a harmonised risk view across the three lines of defence model.

3. **Embed emerging technologies and data analytics**

   To achieve truly integrated assurance, organisations should implement a technology-driven reporting solution. This provides real-time, aggregated reporting across all assurance activities, offering a comprehensive view of progress, outcomes, and remediation status. This enhanced visibility enables more effective monitoring, proactive risk management, and improved decision-making.

Governance

Remuneration

Across the banking, investment and wealth management, and insurance sectors, remuneration continues to be a key area of focus for UK and EU regulators, given the link between risk, reward, and individual accountability.

For banking and investment and wealth management firms, there is a specific UK and EU regulatory requirement that the implementation of their remuneration policies be subject to a central and independent internal review on at least an annual basis. Whilst there is no requirement that this must be carried out by internal audit, many firms leverage their internal audit functions given their independence from remuneration policy implementation. For insurance firms, while not mandatory, such reviews are also highly advisable as they are a key means by which a firm's Board can demonstrate it is discharging its responsibility for the oversight of the implementation of the firm's remuneration policy.

Three things you should know about the topic:

- **Enhanced Prudential Regulation Authority (PRA) expectations for remuneration governance and senior manager variable pay in the banking sector:** The publication of draft amended UK banking sector remuneration rules and regulatory guidance in November 2024 has put firms on notice that the PRA is expecting enhancements in certain areas of remuneration governance (e.g. oversight for Material Risk Taker (MRT) identification and the application of risk adjustment) and in how firms assess senior manager performance for the purposes of determining their variable pay. With the final rules anticipated in Q4 2025, the PRA makes clear that, in determining variable pay, the performance of senior managers against their specific responsibilities should be assessed, including how senior managers have addressed supervisory concerns and actions requested by regulators.
- **Increased EU regulatory focus on local performance and local risk adjustment:** EU regulators in the banking sector (both local regulators and the European Central Bank (ECB) have been actively engaging with firms on how local entity performance and local risk issues are considered when determining variable pay. Given the structure of global bonus pools, non-EU headquartered firms may need to take additional steps to evidence how this is achieved.
- **Potential further divergence between UK and EU remuneration rules:** For firms that navigate the application of more than one set of remuneration rules across multiple jurisdictions, the proposed changes to the UK banking sector rules and further changes expected to the Financial Conduct Authority (FCA) rules in other sectors are likely to create further divergence (e.g. in relation to MRT identification, 60% deferral thresholds and retention periods). Challenges include ensuring that staff who perform group roles are appropriately identified as Material Risk Takers in relation to the different local entities, and that local remuneration requirements (and regulatory expectations) are correctly applied.

Five things internal audit should do:

1. **Tailored remuneration internal audit strategy**

   Internal audit functions should develop a tailored, risk-based remuneration internal audit strategy appropriate to the firm. In some firms, a full review is undertaken each year, but others will look to cover all areas over a rolling three-year period.

2. **Risk adjustment at a bonus pool level**

   Internal audit should review the firm's current documentation relating to risk adjustment to assess whether the firm would be able to demonstrate how all types of current and future risks have been taken into account when determining the bonus pool. Consideration should be given to whether the application of "ex ante" risks (i.e., risks that have not yet crystallised) have been expressly factored in and, where the firm operates multiple jurisdictions considering local risk issues.

3. **Risk adjustment at an individual level**

   The practical application of risk adjustment at an individual level is an area of enhancement. Internal audit should ensure that any adjustments made to "in year" bonuses are communicated clearly to impacted employees.

   Internal audit should assess whether contractual documentation and employee communications make clear that clawback may be applied in relation to non-deferred variable pay, as well as the deferred component, and that express employee acceptance to clawback provisions is obtained.

4. **Application of multiple remuneration rules**

   Where the firm is subject to multiple remuneration ruleset, internal audit should review the approach to identifying Material Risk Takers (MRT) under the different criteria. The maintenance of separate (even if overlapping) MRT lists will support the clear application of different remuneration requirements to individual employees as needed.

5. **Implementation of remuneration policies**

   The documentation around individual performance assessment often requires enhancement (e.g. missing or incomplete performance appraisals or an absence of clear risk-related objectives). The controls for specific forms of variable pay may require enhancement, which could include verifying that severance payments are not being awarded in cases of poor performance or ensuring appropriate oversight for different forms of variable pay being awarded to MRTs.

Environmental, social and governance

Climate and sustainability risk management

While the focus on ESG factors remains highly relevant to financial services organisations, the landscape is evolving, with a potential shift in prioritisation. The Prudential Regulatory Authority's (PRA) consultation paper (CP10/25) significantly raises the bar for climate change risk management, demanding a more robust and integrated approach. The final supervisory statement is expected to be published by the end of Q3 2025. Firms must rigorously assess their capabilities, particularly concerning scenario analysis and the integration of climate risks into broader risk management frameworks. The new UK IA Code of Practice requires assurance over environmental sustainability, climate change risks and social issues such as diversity, equity and inclusion.

Five things you should know about the topic:

- **Integrated climate risk management:** The PRA expects stronger Board oversight, regular reporting on climate risk management practices, and concrete plans to achieve stated targets. Integrating climate risk into risk appetite frameworks using quantitative metrics and limits is crucial.
- **Enhanced climate scenario analysis (CSA):** Firms must improve their CSA and toolkits using conceptually sound models tailored to specific business contexts and incorporating reverse stress tests. Improved Board and management training on CSA methodologies, including the use of more granular data and sophisticated strategical techniques, is essential.
- **Climate-impacted financial reporting:** Financial institutions must explicitly integrate material climate-related risks into their financial reporting, credit loss projections, internal capital and liquidity assessments. This includes assessing the materiality and impact of climate risks on net cash outflows and asset values within liquidity buffers, aligning with international best practices.
- **Global focus on sustainability risk management:** Effective January 2026, these guidelines represent a critical step in the EU's efforts to align the financial sector with the European Green Deal. They set out methodology and minimum standards for identifying, measuring and monitoring sustainability risks. Growing awareness among Asia-Pacific (APAC) regulatory bodies is driving regulatory and oversight efforts to align the region's financial sectors with climate action goals. For example, the Hong Kong Monetary Authority, Japan's Financial Services Agency, and Bank of Japan have conducted climate stress tests and scenario analyses to assess climate change's impact on financial institutions and system stability.
- **Insurer scrutiny:** Insurers must enhance climate risk integration into their Own Risk and Solvency Assessment (ORSA) as per the PRA's recent consultation, ensuring that Solvency Capital Requirements (SCR) calculations accurately reflect climate impacts on claims, asset valuations, and the Matching Adjustment (MA).

Four things internal audit should do:

1. **Robustness of climate scenario analysis**

   Consider integrating a CSA model as part of your model risk management audit strategy, with targeted focus on CSA models, data inputs, and scenario design.

   Assess the explicit integration of climate-related risks into the Internal Liquidity Adequacy Assessment Process (ILAAP) and review the assessment of climate risks' materiality and impact on net cash outflows and asset values.

   Tailoring CSA to firm-specific risk profiles requires significant expertise. Internal audit should drive capability and skills assessments to timely identify potential gaps.

2. **Horizon scanning and impact analysis**

   Regulatory requirements continue to evolve, and divergence could be expected across different jurisdictions. It is critical that the firm has effective horizon scanning procedures in place to monitor new requirements across all relevant jurisdictions and assess the impact of emerging regulations.

   Determine the consistency between the organisation's publicly stated sustainability commitments (including any recent changes or scaling back of commitments) and its actual operational strategies and risk management.

3. **Climate risk into the ORSA**

   Assess the integration of climate risks into the own risk and solvency assessment (ORSA) process for insurance firms, focusing on the accuracy of Solvency Capital Requirement (SCR) calculations reflecting climate impacts on claims, asset valuations, and the matching adjustment.

4. **Data availability**

   The scarcity of granular, reliable data, coupled with the cost and risk associated with third-party reliance, remains a challenge for effective risk management frameworks. Validation of third-party data and the optimal balance between outsourced and in-house data capabilities should continue to be reviewed and challenged.

Environmental, social and governance

Sustainability reporting

The International Sustainability Standards Board's (ISSB), established by the International Financial Reporting Standards (IFRS) Foundation, has issued new standards, raising the bar on corporate reporting related to climate and sustainability performance. These standards primarily focus on companies seeking to access international capital markets and those operating in jurisdictions adopting or endorsing ISSB guidelines. While these standards are currently voluntary in many regions, the UK, Canada, Australia and parts of the EU and Asia are moving towards mandatory adoption, signifying a significant shift towards global consistency in sustainability reporting. The UK is seeking to adopt IFRS S1 and IFRS S2 with some proposed modifications. A consultation is currently underway on the exposures drafts respectively called UK SRS S1 and UK SRS S2.

Five things you should know about the topic:

- **Building on TCFD:** The ISSB's IFRS S2 builds upon the framework established by the Task Force on Climate-related Financial Disclosures (TCFD), adopting its four-pillar structure. A firm's existing TCFD work and compliance with prudential climate risk requirements under SS3/19 are crucial for meeting ISSB Climate-related disclosure requirements.
- **Increased granularity:** The standards mandate disclosures on short, medium, and long-term risks and opportunities across the value chain. This includes granular reporting on greenhouse gas emissions, transition plans, and scenario analysis.
- **Industry specific guidance:** IFRS S2 emphasises the use of industry-specific metrics and disclosure. Companies should consider sector-specific guidance when identifying and managing climate-related risks and opportunities.
- **Aligned disclosures:** The ISSB requires disclosures aligned to the financial reporting cycle. Aligning processes and understanding data requirements will allow you to develop a consistent and more efficient reporting method.
- **Further climate-related targets:** When setting and disclosing climate-related targets, consideration should be given to:

  (i) Alignment with the latest international climate agreements (e.g., Paris Agreement);

  (ii) Third-party validation of targets;

  (iii) Planned use of carbon credits to achieve net-zero targets; and

  (iv) Information on the approach to setting, reviewing, and monitoring progress.

Four things internal audit should do:

1. **Governance and oversight of sustainability reporting**

   Assess the effectiveness of the firm's governance structure and processes related to sustainability reporting.

   Review the board's oversight, the roles and responsibilities of management.

2. **Data reliability and integrity**

   Evaluate the adequacy of internal controls over the collection, analysis, and reporting of sustainability-related data.

   Assess the firm's commitment to the accuracy and completeness of its disclosures.

   Evaluate the controls around data sources, data quality checks, and data aggregation.

   Evaluate the methodologies used for calculating emissions (Scope 1, 2, and 3) and the validation of any third-party data used.

3. **Compliance with ISSB Standards**

   Evaluate the firm's compliance with the ISSB standards, including the completeness and accuracy of disclosures related to climate-related risks and opportunities, transition plans, and targets.

   Many firms are currently developing their aligned assurance strategies. This presents opportunities for aligned assurance, where internal audit can coordinate its work with assurance provided within the firm to improve efficiency and provide a more holistic view of the firm's sustainability performance and reporting.

4. **Target setting and monitoring**

   Evaluate the adequacy of inputs across the climate-related target setting.

   Verify the accuracy of reported progress against targets, i.e. MI and analysis and challenge suitability of key triggers and decision-making tools.

Digital risk and change

Change and transformation

The global financial services sector is experiencing a market evolution, driven by the rapid adoption of GenAI solutions and a surge in market consolidations and reorganisation particularly within the insurance and banking sectors. Furthermore, ongoing geopolitical uncertainties have introduced considerable volatility into global markets, increasing risk profile, impacting investor confidence and forcing Boards to refocus investment on short term and defensive capabilities.

Internal audit functions should continue to challenge the change strategy, focusing on the effectiveness of return on investment and cost reduction for major changes, strategic alignment of change objectives during transition to BAU and the integration of GenAI technologies.

Five things you should know about the topic:

- **Ensuring success – a cost-effective approach to change management:** Uncertainty in the markets (and related revenue-generating opportunities) leads a business to focus on more controllable elements of business performance, such as the prudent management of costs. This involves integrating diverse resource models (including offshore), lean delivery, and technology. Risk managers and change assurance teams should identify and track the critical success factors, such as achieving clear outcomes for customers, employees, and regulators.
- **Navigating the challenges of 'as-a-service' transition:** The rapid adoption of 'as-a-service' solutions can leave customers and support unprepared, leading to change programmes not meeting their objectives during the transition to live operations. The internal audit function faces the challenge of not only providing oversight, but to advocate for customer experience, challenging the practicality of new solutions.
- **Balancing agile delivery with talent retention:** While agile and value stream change delivery methods drive innovation, retaining in-house expertise remains a challenge. Over-reliance on third parties, coupled with inconsistent agile application, can lead to wasted resources and drawn-out implementation timescales.
- **Navigating the regulatory shift:** The push for streamlined financial regulations in pursuit of economic growth and enhancing competition in the market presents a risk to end customers. The response of the change portfolio and product owners should be to create an environment conducive to progress without compromising the safety of customers.
- **Change programme pitfalls: Why transitions to BAU often fail:** Many change programmes struggle to fully realise their objectives during the transition to business-as-usual (BAU). Old problems resurface, hindering the intended benefits and highlighting the need for improved handover processes and more robust change management strategies.

Five things internal audit should do:

1. **Strategic approach**

   Internal audit should strategically assess change by considering key milestones and applying proportionate controls based on its nature and scale. Crucially, they must evaluate whether their assurance coverage remains fit for purpose.

   Aligned with CIIA Code of Practice, internal audit activities must align on key corporate events (e.g., business process changes, new products/services, M&A activity).

2. **Governance**

   Internal audit should expand its role beyond assessing the change execution. It must actively examine business strategy, challenge existing practices, and proactively assess the risks of inaction, with a stronger emphasis on governance oversight.

3. **Skills versus skilled**

   Digitisation has increased reliance on external expertise for business transformation. Future-proof skills include using tools and GenAI technologies to automate development and other processes. Internal audit should review talent management and challenge future workforce strategies.

4. **Quality of reporting and data**

   Cost-cutting on change initiatives drives the need for internal audit to evaluate the appropriateness of objectives and key results (OKRs), quality of management information, stakeholder awareness, and risk management.

5. **Never a failure, always a lesson**

   Post-implementation reviews often prioritise large transformations, but continuous improvement, like DevOps, is key for long-term sustainability. Internal audit should ensure the organisation benefits from a centralised lessons-learned repository, especially learning from programmes that involve group level and local stakeholders.

Digital risk and change

Operational resilience

While the UK regulatory deadlines have now passed, operational resilience remains a key area of focus for firms, and internal audit functions alike. It is imperative that any momentum built up to the regulatory deadline is not lost. In an uncertain and constantly evolving landscape, firms need to remain alert to new vulnerabilities and ensure that important business services remain resilient. Recent large-scale disruptive events highlight the continued importance in building a resilient business that can respond and recover from a range of expected disruptions. How will geopolitical instability sanctions, trade wars, or unforeseen global events impact an organisation's ability to operate? This requires a more sophisticated approach to scenario planning than previous years.

Four things you should know about the topic:

- **A holistic approach to operational resilience**: The focus up to the Prudential Regulation Authority (PRA) regulatory deadline has understandably been on achieving regulatory compliance. There is a need for firms to understand and draw upon wider resilience capabilities such as business continuity and disaster recovery and third-party risk management, for which firms have often run separately to operational resilience programmes.
- **Effective communication to navigate disruptions**: High-profile disruptions in early 2025 alone highlight the importance of robust and effective communication strategies to manage both internal and external stakeholders, to reduce any potential negative impacts as much as possible. Strategies to support communication internally to staff and external stakeholders such as the media (including social media), suppliers, customers, and the regulator should be designed and regularly tested to provide management with assurance over its useability and continued effectiveness.
- **Enhancing MI to support resilience efforts**: Management information (MI), although not a new area of focus, is still a weak area for many organisations and requires continued development and maturity to enable boards to apply appropriate governance over operational resilience activities. Effective and timely MI and reporting will support resilience investment decisions, so it is imperative that appropriate MI is in place.
- **Building a proactive culture of resilience**: One of the key aims of the regulation was to drive a cultural shift in how firms view operational resilience, by embedding resilience considerations in the day-to-day running of the business and operational processes. In the past, resilience has been as a by-product of investment into systems, processes and controls. However, management now needs to put resilience first – as the desired outcome – and systems, processes and controls should be developed to maximise the resilience of a firm's most important business services.

Five things internal audit should do:

1. **Assessment of wider resilience capabilities**

   Internal audit functions should assess their organisation's approaches to resilience beyond the regulatory requirements. Traditional areas such as business continuity, IT disaster recovery, and third-party risk management should be subject to review through the resilience lens to ascertain the end-to-end resilience capability. Technology resilience by design should be a key area of focus, given the advent of AI and automation, cloud security and quantum computing threats.

2. **Communications strategies**

   The robustness and useability of both internal and external communications strategies should be subject to scrutiny by internal audit, particularly in the context of understanding how they can be leveraged in the event of a disruption to minimise fallout and help to facilitate a stronger recovery.

3. **Embedding a culture of resilience**

   Internal audit activity should focus on resilience across the broader audit plan, considering whether resilience controls and associated risks are adequately embedded across a range of audits that impact important business services, both directly and indirectly

4. **Management information**

   Internal audit functions should continue to apply challenge to the quality and effectiveness of MI to ensure it is – and continues to be, in light of business change - appropriate for business needs. For example, they should challenge management on the use of data-driven insights to identify emerging risks and trends, using key risk indicators (KRIs) and key performance indicators (KPIs) to monitor operational resilience, and encourage the move beyond reactive reporting to proactive insights on emerging risks and opportunities.

5. **Embedding of operational resilience activities into BAU environment.**

   Focus needs to continue to be put on supporting areas of activity within businesses. In particular, existing technology resilience processes may need to be re-engineered, so they effectively support wider operational resilience outcomes. Change methodologies and controls should adequately dovetail into the operational resilience landscape, ensuring firms' resilience frameworks and practices are systematically refreshed and updated.

Digital risk and change

Third Party Risk Management (TPRM)

The escalating complexity of global supply chains, coupled with unpredictable macroeconomic and geopolitical shifts, has amplified the vulnerability of organisations reliant on third-party services. Cyber-attacks, data breaches, and compliance failures are no longer hypothetical threats; they are frequent occurrences crippling businesses. The lack of reliable, accurate information from third and fourth parties further exacerbates the problem, leaving many TPRM programmes struggling to keep pace.

Six things you should know about the topic:

- **Intensified financial services sector regulatory requirements:** The UK's Critical Third Party (CTP) Oversight Regime and the EU's DORA, both effective in early 2025, significantly increase the complexity of financial services regulation, requiring firms to navigate distinct but overlapping requirements for managing critical third-party relationships, focusing on business continuity (UK) and information and communication technology (ICT) provider regulation (EU). Stringent regulations and increased third-party disruptions are driving large-scale remediation efforts. Common compliance challenges include responding to large-scale remediation efforts across multiple divisions and geographies, as well as understanding the baseline for regulatory compliance across various regulations.
- **Emerging artificial intelligence (AI) risks in third-party relationships:** The increasing use of GenAI tools, both internally and by third parties, requires a sophisticated TPRM framework to address emerging risks. This includes data quality, algorithm reliability, cybersecurity, data privacy, and ethical considerations to mitigate potential operational disruption and reputational damage.
- **Operational resilience and TPRM:** Organisations must continue to integrate operational resilience with third-party risk management capabilities to meet the growing regulatory requirement. This ensures that third-party disruptions do not exceed acceptable impact thresholds.
- **Third party governance:** A robust governance structure for third-party risk management is essential for accountability, consistent policy application, effective monitoring, proactive risk mitigation, regulatory compliance, and transparent communication. It ensures that roles are clearly defined, risks are consistently identified and addressed, and the organisation demonstrates a commitment to managing third-party risks effectively.
- **Use of risk intelligence over traditional attestation-based assurance:** The traditional attestation-based and point-in-time approach to third-party risk assessment relies heavily on self-reported data, limiting its effectiveness. Increasingly, organisations are adopting risk intelligence, leveraging external data sources and advanced analytics to gain a more comprehensive and objective view of third-party risks. This shift allows for proactive identification of emerging threats and vulnerabilities, moving beyond reactive compliance checks to a more predictive and resilient risk management strategy.
- **IIA topical requirements:** The Institute of Internal Auditors (IIA) is expected to finalise their topical requirements on Third-Party risk, later this year, which will be mandatory for internal audit functions.

Five things internal audit should do:

1. **Intensified financial services sector regulatory requirements**

   Effective collaboration across all three lines of defence and consistent internal audit involvement is crucial to ensure the business and risk areas have considered the changes in the regulatory environment and uplifted policies and processes accordingly.

2. **Emerging AI risks in third-party relationships**

   Internal audit may provide independent assurance on the effectiveness of controls mitigating AI-related risks within third-party relationships, encompassing data governance, cybersecurity, and compliance; this includes evaluating due diligence processes, monitoring performance, and reporting on emerging threats to management and the board.

3. **Operational resilience and TPRM**

   Internal audit may evaluate the impact of third parties on the organisation's ability to remain within its impact tolerance limits by assessing the consideration of third-party failures in stress testing scenarios and reviewing the robustness of business continuity plans (BCPs) and exit strategies for critical third parties, ensuring alignment with the organisation's overall BCP.

4. **Third party governance**

   Senior oversight is essential for all successful TPRM programmes and internal audit has a key role to play as the third line in the governance structure for TPRM in any financial services organisation, through proactive audit planning and identification of key roles and responsibilities within the TPRM governance structure.

5. **Use of risk intelligence over traditional attestation-based assurance**

   Internal audit should test the effectiveness of risk intelligence outputs, including feeding into the effectiveness of large-scale technology implementations in third-party risk management, by reviewing data sources and methodology, comparing results with traditional attestation methods, testing predictive capabilities, assessing alerting mechanisms, reviewing governance and controls, and interviewing key personnel. This multifaceted approach helps determine the reliability and value of the organisation's risk intelligence programme.

Digital risk and change

Cyber risk

In an era defined by digital acceleration and systemic unpredictability, cyber security has transcended its traditional boundaries to become a cornerstone of enterprise resilience. The cyber security landscape is in constant flux, with new threats and vulnerabilities emerging daily.

For internal audit functions, staying ahead of the curve is critical to ensuring the effectiveness of their risk management and assurance activities. Proactive review and challenge of internal security controls, and continuous monitoring are essential for navigating the complex and ever-changing cyber security landscape.

Five things you should know about the topic:

- **Artificial intelligence (AI) is rapidly transforming the cyber threat landscape:** Attackers are leveraging AI for automated phishing campaigns, sophisticated malware development, and the rapid identification of vulnerabilities. This necessitates a shift towards AI-driven security solutions for detection and response.
- **Human error remains a significant cyber security vulnerability, despite technological advancements:** The 2025 attacks on major retailers highlight this, showcasing sophisticated techniques using advanced social engineering, custom malware. and modified leaked ransomware code. Robust security measures, including multi-factor authentication, endpoint detection and response (EDR), data loss prevention, and comprehensive security awareness training, are vital for mitigating these threats. Recent attacks such as that on insurers in the US, where hackers stole personal information from customers, highlight that this is global risk. Robust security measures, including multi-factor authentication, endpoint detection and response (EDR), data loss prevention, and comprehensive security awareness training, are vital for mitigating these threats.
- **Cyber-attacks targeting the supply chain are becoming increasingly prevalent:** Organisations need to assess and manage the cyber security risks associated with their third-party vendors and suppliers. This requires robust due diligence processes and ongoing monitoring of vendor security practices.
- **Cyber and the Internet of Things (IoT):** The expanding attack surface of IoT and Operational Technology (OT) devices presents significant cyber security risks. The sheer number and diversity of these devices, often lacking robust security features, creates numerous entry points for attackers. Legacy systems, outdated protocols, and insufficient network segmentation exacerbate vulnerabilities. The potential for cascading effects from a single compromised device necessitates a comprehensive and proactive approach to security.
- **IIA topical requirements:** The Institute of Internal Auditors (IIA) has released a cyber security topical requirement in Q1 of 2025, providing a baseline approach for assessing cyber security governance, risk management, and control processes. Internal audit functions must understand and comply with these requirements when conducting cyber security audits or when cyber security is identified as a risk within other audits.

Five things internal audit should do:

1. **Assess the maturity of cyber security programmes**

   Internal audit should evaluate the maturity of the organisation's cyber security programme against recognised frameworks such as NIST cyber security framework. This assessment should focus on the effectiveness of people, process and technology in mitigating identified risks.

2. **AI attacks**

   Internal audit must assess the organisation's readiness for AI-powered attacks. This involves evaluating AI-powered threat detection systems, deepfake detection technologies, and employee awareness. A crucial aspect is reviewing the security implications of AI deployment across all systems and processes, ensuring robust AI-related security practices are in place to mitigate risks.

3. **The evolving threat of ransomware**

   Internal audit should verify the effectiveness of security awareness training (including phishing simulations), assess the security culture, and confirm robust access controls. A comprehensive vulnerability management programme (patching, scanning, penetration testing) and strong data security measures (classification, encryption, DLP) are crucial. Finally, the incident response plan needs regular testing and updates to ensure effective communication and recovery.

4. **Supply chain security**

   Third-party vendor reliance expands cyber security risk. Internal audit should review supplier risk assessments, enforcing robust cyber security clauses in contracts, and monitoring the entire supply chain's security posture. This proactive approach strengthens overall security and resilience.

5. **IIA cyber security topical requirement compliance**

   The IIA's cyber security topical requirement (released in Q1 of 2025) will become mandatory for audit engagements. Internal audit should prioritise achieving and maintaining compliance with this requirement. This involves collaborating with information/cyber security teams to improve cyber security risk assessments, enhance the controls environment, and develop a robust technology strategy. The focus should be on aligning audit processes with the new standards and ensuring ongoing conformance.

Digital risk and change

Data governance

Data remains a strategic asset, but inadequate governance creates a significant competitive disadvantage, hindering innovation and efficiency while raising costs and reputational risks. The rapid growth of data and accelerating technological change (e.g., changes in the AI landscape) exacerbate this challenge, further amplified by the increasing reliance on data-driven decision-making across all business functions. This is reflected in data's rise as one of the critical topics for internal audit functions.

Five things you should know about the topic:

- **Sustained and accelerated technological change:** The rapid pace of technological innovation creates a significant challenge for organisations to keep pace with evolving data security threats and best practices. This widening gap necessitates a more urgent focus on embedding data management practices and data governance frameworks. The migration of data to the cloud introduces new risks related to data security, privacy, and compliance.
- **Data management, privacy, and security regulations:** The regulatory landscape surrounding data privacy and security is dynamic, requiring organisations to adapt quickly and maintain ongoing compliance. While UK law relies on existing legislation to help govern the changing technology landscape, there are increasing principle-based guidance which organisations need to navigate which can create uncertainty around compliance. Regulations like GDPR in EU, California Consumer Privacy Act (CCPA) in the US, and others are constantly evolving and becoming more stringent.
- **Sustainable data maturity:** Achieving robust data governance is a journey, not a destination. Organisations are starting to focus on sustainable maturity, building capabilities incrementally and fostering a culture of continuous improvement. "Walking before running" is key.
- **Digital savviness and leadership:** A strong commitment to data governance must be driven from the top. Successful organisations set the tone at the top to champion digital literacy and foster a culture of data responsibility throughout the organisation.
- **Data resilience and business continuity:** Organisations need to build data resilience into their operations to ensure business continuity in the face of disruptions, whether caused by cyberattacks, natural disasters, or other unforeseen events.

Five things internal audit should do:

1. **Prioritise and guide data governance initiatives**

   Internal audit should collaborate with the business to identify and prioritise key initiatives, offering practical guidance and risk assessments to bridge capability gaps and achieve sustainable maturity. Focus should be on incremental, achievable improvements.

2. **Champion a culture of continuous improvement**

   Internal audit should promote the implementation of a continuous monitoring programme for data governance, including regular data quality assessments and process reviews. Based on the findings, specific improvement recommendations should be developed and implemented iteratively. A feedback loop should be established to track progress and ensure ongoing improvement.

3. **Promote data literacy and digital savviness**

   Internal audit should champion data literacy training programmes, starting with senior leadership, to foster a culture of data responsibility and informed decision-making at all levels.

4. **Proactively assess emerging data risks**

   The use of emerging technologies, automation, data analytics, and AI for decision making requires strong data quality and data management processes. Internal audit needs to assess the risks associated with automated systems and ensure data quality throughout the automation lifecycle.

5. **Strengthen data resilience and business continuity**

   Internal audit should assess the organisation's data resilience by evaluating its data protection and recovery mechanisms. This includes reviewing data backup and recovery procedure, disaster recovery plans, and incident response strategies for data-related incidents. This should include consideration of adherence to recovery time objectives (RTOs) and recovery point objectives (RPOs).

Digital risk and change

Cloud

While cloud adoption continues unabated, the landscape is evolving rapidly. With a significant proportion of UK organisations' IT estates still hosted in on-premises environments, there is still some way to go in many organisations' journeys to migrate to cloud.

This year's focus should be on two key evolving trends significantly impacting risk management. Firstly, the rise of data sovereignty and national security concerns is leading to a more fragmented cloud landscape. Increasing regionalisation of the cloud market, driven by geopolitical factors and specific regulations like GDPR, California Consumer Privacy Act, the Singapore Personal Data Protection Act, creates potential vulnerabilities. Secondly, environmental, social, and governance (ESG) factors are gaining significant traction in cloud strategies. Organisations must now consider the environmental impact of their cloud consumption (e.g., carbon footprint), ethical sourcing of technology, and the broader societal implications of their cloud deployments.

Four things you should know about the topic:

- **Geopolitics and impact on the cloud:** Increased geopolitical tensions are driving a trend towards regionalisation of cloud services. This necessitates a thorough assessment of data sovereignty implications, including compliance with varying national regulations (e.g., GDPR, CCPA, CDSA) and the potential for data breaches or restrictions on access. Furthermore, organisations must consider the risks of vendor lock-in, limiting flexibility and potentially increasing costs, and the potential for service disruptions stemming from escalating international relations or geopolitical instability. A robust risk mitigation strategy should address these interconnected challenges, ensuring business continuity and data security in a volatile global landscape. This strategy should include diversification of cloud providers, robust data governance policies, and comprehensive incident response plans.
- **ESG is a business imperative:** Organisations must integrate ESG factors into their cloud strategies, considering energy consumption, carbon footprint, and ethical sourcing of cloud services. This includes due diligence on cloud providers' sustainability initiatives.
- **Cloud and data responsibility:** With increased cloud adoption comes increased responsibility for data security and privacy. Regulations like the UK GDPR and EU Network and Information Security Directive 2 (NIS2) continue to evolve, demanding robust security controls and compliance frameworks.
- **Resilience of cloud supply chains:** Organisations must assess the resilience of their cloud supply chains. Dependencies on specific providers can create vulnerabilities. Diversification and robust vendor management strategies are crucial.

Five things internal audit should do:

1. **Assess geopolitical risk impact to the cloud ecosystem**

   Internal audit should assess the organisation's exposure to geopolitical risks related to cloud providers. This includes evaluating data sovereignty compliance, vendor concentration, and potential service disruptions.

2. **Integrate ESG into cloud audits**

   Internal audit should incorporate ESG considerations into its cloud audits, evaluating the organisation's cloud strategy against its ESG goals and assessing the sustainability of its cloud providers.

3. **Enhance data security and privacy reviews**

   Internal audit should strengthen its data security and privacy reviews, ensuring compliance with evolving regulations like the UK GDPR and NIS2. This includes testing access controls, data encryption, and incident response plans.

4. **Review supply chain resilience**

   Internal audit should assess the resilience of the organisation's cloud supply chain, identify potential vulnerabilities and recommend mitigation strategies. This includes evaluating vendor diversification and contract terms.

5. **Monitor cloud costs**

   Internal audit should regularly monitor cloud costs, identifying areas for optimisation and recommending cost-saving measures. This includes reviewing resource utilisation, identifying inefficiencies, and leveraging cloud cost management tools.

Internal audit innovation and transformation

GenAI usage across internal audit lifecycle

In 2024, we explored the transformative potential of Generative AI (GenAI) for internal audit. Fast forward one year, and we're witnessing a remarkable surge in GenAI adoption across the industry. Our clients have highlighted tangible improvements in efficiency and quality, and impact is being realised throughout the audit lifecycle. Our latest research indicates that approximately 79% of internal audit functions are now utilising tools like Co-pilot, with a further 38% exploring custom-built GenAI solutions.

While many functions are still in the early stages – primarily leveraging chatbots and in-house wrappers around Large Language Models (LLMs) – a clear shift is underway towards more tailored GenAI applications and seamless integration with existing systems. Applications are expanding beyond initial risk assessment and audit planning to encompass automated testing, working paper drafting, report generation, issue tracking, resource scheduling, and even tailored learning paths for audit teams. The market is seeing a rise in several types of GenAI tooling, including enterprise tools (like ChatGPT and Co-pilot), agentic ecosystems, specialised GenAI (such as Deloitte's Internal audit and controls hub and Co-pilot integrations), and AMS GenAI (e.g., AuditBoard). These tools range in design from end-user driven to workflow-based and platform-embedded solutions.

Five things you should know about the topic:

- **Maturing adoption and practical deployment:** GenAI is moving beyond the hype cycle towards pragmatic, integrated deployment. The focus is shifting to secure, tailored solutions and effective integration with existing systems.
- **Elevating the auditor's role:** GenAI augments, not replaces, auditors. By automating routine tasks, it frees up time for higher-value activities like critical thinking, strategic insights and partnering with the business to identify the right response to audit findings. Robust human oversight - "human in the loop" remains crucial to mitigate risks such as "hallucinations" and bias.
- **Data strategy as a foundation:** The success of GenAI in audit depends on high-quality, accessible data. A comprehensive organisational data strategy is essential, encompassing proactive data curation, accuracy, security, and the potential use of synthetic data.
- **Navigating regulatory and ethical landscapes:** Internal audit in financial services must stay abreast of evolving AI regulations (e.g., EU AI Act, FCA guidance) and ethical considerations. Assurance over fair, transparent, and explainable GenAI deployments is paramount.
- **Upskilling and mindset shift:** Harnessing GenAI requires significant upskilling in AI concepts and prompt engineering. A cultural shift is also needed to embrace AI as a collaborative tool, fostering a new approach to teamwork and leveraging intelligent tools effectively.

Five things internal audit should do:

1. **Develop a tailored GenAI strategy**

   Create a GenAI strategy identifying high impact use cases and set clear objectives for phased integration into audit processes. Consider the available technology i.e. enterprise (e.g., ChatGPT, Co-pilot), specialised (e.g., Deloitte's IA&C Hub), and AMS GenAI (e.g., AuditBoard), and select a design (end-user driven, agentic, workflow-based, or platform-embedded) that aligns with your organisation's capabilities and strategic goals. Prioritise secure, scalable implementation and define how success will be measured i.e. improved efficiency, quality and impact.

2. **Establish robust AI governance**

   Implement comprehensive governance for GenAI, encompassing policies for data privacy, model validation, output accuracy, and ethics. Ensure clear "human-in-the-loop" protocols for accountability. This governance framework should address the specific risks associated with the chosen GenAI tools and their integration into existing systems.

3. **Build a strategic data foundation**

   Collaborate with data teams to identify, curate, and prepare high-quality datasets for GenAI. Address data integrity and quality issues proactively to maximise effectiveness and minimise risks.

4. **Invest in upskilling and culture**

   Prioritise continuous learning for auditors on GenAI fundamentals and risks in addition to the skills needed to critically evaluate and challenge GenAI outputs, ensuring that the 'human in the loop' remains an effective and integral part of the process.

5. **Pilot and scale responsibly**

   Focus initial GenAI efforts on specific, high-value use cases in controlled environments. Successful piloting builds confidence and demonstrates ROI, paving the way for broader deployment.

Internal audit innovation and transformation

Data analytics

The past year has seen a dramatic shift in the urgency surrounding data analytics for internal audit. While the importance of data-driven insights has been discussed for years, 2026 marks a turning point: the sheer volume and velocity of data, coupled with increasing regulatory demands and stakeholder expectations, have made data analytics a non-negotiable for maintaining relevance and effectiveness. To succeed, internal audit functions must adopt a multi-faceted approach encompassing a well-defined strategy, comprehensive data literacy training, proactive data quality assessments, compelling communication of insights, and a robust plan for implementing Continuous Controls Monitoring (CCM). This proactive approach will enable internal audit to deliver greater value and enhance its contribution to the organisation.

Five things you should know about the topic:

- **A strategic approach is paramount:** Aligning analytics plans with the overall strategy of the function is crucial for success. Our 2025 internal audit data and analytics survey revealed that 90% of functions with aligned strategies reported successful analytics implementation, highlighting a strong correlation between strategic alignment and positive outcomes.
- **Data literacy is a core skill:** Strong data literacy empowers audit teams to derive accurate insights, make informed decisions, and build greater stakeholder trust. However, our survey revealed a significant gap: while 62% of functions provided basic analytics training, with the intention of increasing data literacy across the team, only 3% offered advanced training to a comparable number of staff. Bridging this gap is critical for maximizing the value of data analytics.
- **Data quality requires proactivity:** While 79% of functions evaluate data quality before analysis, a significant 52% still cite poor data quality as a major barrier. This highlights the need for proactive data quality management strategies, not just reactive evaluation, to ensure the reliability and accuracy of audit findings. Internal audit should continue to articulate the risk to the business and provide recommendations to support improvement in this space.
- **Effective storytelling is essential:** Communicating data-driven insights effectively is crucial for stakeholder engagement and decision-making. Visualisations, compelling narratives, and regular progress reporting are essential for translating complex data into actionable information. We have noted that functions who have better uptake when implementing new tooling, particularly GenAI, have been good at sharing success stories within team.
- **Continuous Controls Monitoring (CCM) requires clarity:** While the value of CCM is widely recognised, its optimal placement within the three lines of defence remains a subject of debate. The key to successful CCM implementation is clear definition of objectives and a well-defined process for translating insights into actionable steps.

Five things internal audit should do:

1. **Assess maturity, set realistic goals**

   Clearly define your ambitions and current capabilities. Conduct a self-assessment to identify your current maturity level and set measurable goals aligned with your resources and capacity for growth.

2. **Develop a robust analytics toolkit**

   Continuously evaluate and enhance your analytical toolkit to incorporate the latest technologies and techniques, such as generative AI, advanced processing, and effective visualisation tools.

3. **Integrate with existing systems**

   Streamline data access and reduce lead times by integrating analytics tools with existing audit management systems and data warehouses. This improves efficiency and reduces the risk of errors.

4. **Build a high-performing analytics team**

   Proactive communication between analytics and audit teams is key to effective data analytics. Invest in a skilled team that translates requirements into tests and insights into actionable recommendations, fostering collaboration and providing targeted training for clear communication and effective data storytelling.

5. **Foster a culture of continuous improvement**

   Embrace experimentation, feedback, and iterative refinement to ensure your data analytics initiatives remain effective and adaptable in a constantly evolving landscape. Stay current with industry trends and best practices to maintain a competitive edge.

Internal audit innovation and transformation

A high performing internal audit function

Impactful audit functions need to not just adapt but thrive in the face of ongoing change and disruption. Regulatory changes, digital transformation, organisational restructuring, shifts in target operating models, offshoring and the complexities of mergers and acquisitions — these aren't challenges; they're opportunities to forge a High-Performing Culture (HPC) that helps maximise the value which internal audit provides to its stakeholders.

Five things you should know about the topic:

- **Purpose-driven performance**: Our vision of the value-adding audit function of the future is one which is purpose-driven and digitally powered. The importance of a clear and shared purpose cannot be overstated in helping functions navigate change and disruption whilst maximising the value they add to their organisations.
- **Future-proofing IA culture**: To remain effective, internal Audit (IA) must build resilience to adapt to significant change events such as a change in leadership, shifts in strategic direction, or mergers and acquisitions. Thriving in today's environment requires recognising that change is not an exception but a constant. This means building the capacity within leaders and teams to navigate it effectively by fostering behaviours that enable confidence and fluidity. While this shift takes time and sustained effort, embedding these practices ensures internal audit continues to deliver value amidst disruption.
- **Connecting teams in hybrid environments**: A high-performing hybrid workforce requires strategic talent management: upskilling, reskilling, addressing skill gaps, and offering compelling career paths. As teams continue to explore onshore, near shore and offshore location plans, maintaining consistent quality control and training across geographically dispersed teams demands a carefully considered approach.
- **Championing innovation**: Internal audit must champion continuous improvement and innovation, establishing structures for idea generation, experimentation, and execution across integrated teams. This involves experimenting with new technologies, sharing best practices, and ensuring technology enhances, not replaces, human skills.
- **The human touch in technology**: We expect to see a shift of auditors' responsibilities - previously focused on defining risk and controls (e.g., RACMs), auditors now play a more critical role in challenging the output and managing stakeholder relationships to maximise value. Experimentation where teams explore new tools, share successes, and remember technology should augment, not replace, human skills and judgment.

Five things internal audit should do:

1. **Craft a compelling shared purpose statement**

   Collaboratively, as a function, crafting a purpose statement reflecting the function's mission fosters belonging and shared ownership. Designing innovative performance measures will highlight individual contributions.

2. **Implement a proactive cultural integration plan**

   When considering offshoring or operating during an M&A, implement a proactive cultural integration strategy that anticipates and addresses complexities of change.

   A thoughtful approach, addressing communication styles and technology platforms, creates a united, high-performing team, enhancing audit quality and stakeholder confidence.

3. **Develop a strategic talent management plan for a thriving hybrid and global workforce**

   To ensure consistent service delivery, establish clear communication protocols, utilise visual workflow tools, hold purposeful virtual meetings, and invest in cross-cultural communication training. Well-defined work agreements and a focus on joint accountability and team rewards, rather than individual achievements, foster collaboration and shared success.

4. **Cultivate disciplines for continuous improvement and innovation**

   Innovation should be promoted by all teams. This inclusive approach is key because it leverages the diverse perspectives and experiences of the entire workforce.

   Establishing structures that support this collaborative innovation process, and crucially, leadership giving explicit permission and actively fostering a culture of experimentation, will position internal audit to lead the business through transformation.

5. **Prioritise user experience in your technology strategy**

   When designing and rolling out technological change do not forget the user experience. An approach centred around the people using the technology which fosters experimentation and ensures technology enhances human skills. A well-defined technology strategy focused on innovation and efficiency will enhance collaboration, boost transparency, and deliver faster, higher-quality insights.

Internal audit innovation and transformation

Standards and quality assurance hotspots

The revised Institute of Internal Auditors (IIA) Global Internal Audit Standards ('Standards') and UK Internal Audit Code of Practice ('Code') continue to evolve with new mandatory topical requirements being consulted on and launched across the course of 2025. Although many functions conducted readiness assessments for the new Standards during 2024, audit methodologies and QA practices must continue to evolve as teams look to increase their impact on their broader organisations.

Five things you should know about the topic:

- **Topical requirements: Are you ready?** Topical requirements are a new mandatory component of the Internal Professional Practices Framework which, depending on a function's risk assessment results, must be applied when providing assurance services. Topical requirements on cyber security, third parties and organisational behaviour have been released/consulted on during 2025.
- **Setting your quality target:** The IIA's quality assessment manual now offers two 'pass' grades for the Standards: "General" and the new "Full" conformance, signifying complete adherence to all principles, standards, and requirements. With a significant increase in requirements under the new Standards, functions should determine their desired level of conformance with their audit committee.
- **Measure what matters:** The requirement under Domain IV for an internal audit strategy has driven a focus on a longer-term functional vision with clearly defined, purpose-driven outcomes. Defining meaningful performance measures that monitor both progress and the impact of the strategy remains a key focus for improvement.
- **Beyond compliance - unlocking QAIP's potential:** The higher conformance bar necessitates more efficient and impactful practices. Rapid technological advancements, including Generative AI (GenAI), offer opportunities to unlock efficiencies and expand the scope of Quality Assurance and Improvement Programme (QAIP) activities beyond basic compliance.
- **Code compliance:** The new Code was largely based on the previous Code for Financial Services and so has not posed a significant challenge for many financial services functions. Functions must also consider new priority risk areas, transparency of reporting in the annual report, team diversity approaches, and the Code's inclusion in External Quality Assessment review.

Five things internal audit should do:

1. **Evolve methodologies in response to new topical requirements**

   Topical requirements become effective 12 months after they have been issued. The cyber requirements will become effective from February 2026. Internal audit teams will need to integrate these into methodologies and develop awareness to ensure conformance. In areas such as organisational behaviour, this is likely to be an uplift for many functions.

2. **Set appetite for Standards conformance**

   Internal audit functions should have a view on any gaps to achieving "Full" conformance and understand the effort and benefits of achieving this. Discussion should be held with the audit committee on the appetite for "Full" versus "General conformance".

3. **Define performance measures which measure outcomes as well as inputs**

   Measuring performance against strategic goals with regular touchpoints with key stakeholders will help drive functions to achieve their longer-term visions. Balanced scorecards should be developed which go beyond traditional operational measures to monitor the outcomes and impact of strategic initiatives.

4. **Extend QAIP scope**

   Assess whether QAIP scope is in line with the new Standards and Code. Consideration should be given to areas such as governance reporting, action closure validation, and annual risk assessment and audit planning processes.

   To ensure QAIP adds value, expand your definition of audit quality beyond conformance with methodologies and checklists to include the quality of insight and impact aligned to the internal audit strategy.

5. **Stretch and digitise QAIP approach**

   Is your QAIP approach aligned with your internal audit strategy digital ambitions? Does it contribute to team learning and continuous improvement in this area?

   Identify opportunities to use digital technologies in the QAIP process including GenAI in file reviews and leveraging functionality in audit management systems for continuous QA monitoring.

Internal audit innovation and transformation

Lessons from the field - building the audit function of the future

In March 2025, Nick Curle, Chief Audit Executive of NatWest participated in Deloitte's Heads of Internal Audit community forum, where an interview was conducted with him on the future of internal audit. Nick is leading a team of around 450 auditors since 2021. He has navigated significant change over that period and argues passionately for real-time, adaptive audit functions adding value in a digital world. Highlights from the interview with him are summarised below.

How should internal audit evolve beyond a focus on risk and controls and why is this crucial?

What makes internal audit as a profession valuable and successful today won't cut it tomorrow. Internal audit has an even more interesting and valuable role to play in helping firms win for their customers and stakeholders than it has had up to now. This involves asking broader questions about the achievability of strategies and forward business plans beyond the safety, soundness, and compliance-focused questions traditionally addressed.

At its heart, this is about using evidence available today to challenge outcomes in the future. This involves more uncertainty and needs even better evidence and more judgement than the work has always done. There are some methodology and skills expansions needed for all professionals, but these are manageable. The bigger challenge will be the bravery required as we adapt.

What new or different skills will auditors need?

Two key areas are crucial.

The first encompasses technology, data, analytics, and AI. This is already core but will undoubtedly become pervasive going forward. Everyone needs to improve in this area.

For example, we have gone from having a data analytics team of under 20 to having 100 people across the function, who are considered expert or intermediate in SQL, 80 proficient in Python and 50 in prompt engineering. This upskilling generates more ideas, scales successful innovation experiments, and boosts confidence. We are continually upskilling and aim to have the whole function more proficient in AI and data in the next 12 months.

The second area is business commerciality. Everyone needs to understand exactly how their work affects customers and contributes to the firm's economics; otherwise, effective challenges cannot be made. This represents a significant improvement, moving us from asking from "how safely" to "how well".

> *'Internal audit has an even more interesting and valuable role to play in helping firms win for their customers and stakeholders than it has had up to now.'*

Nick Curle
Chief Audit Executive
NatWest

Internal audit innovation and transformation

Lessons from the field - building the audit function of the future

The new CIIA code broadens the focus from risk and control culture to organisational culture. What role should the internal audit function of the future play?

Organisational culture and colleague behaviour are foundational to our work – you can't decouple effective risk management from organisational culture and behaviours. Findings relating to behaviours are central in many of the themes that we report on to our Audit Committee – we don't view this as a "nice to have" or of secondary interest.

Over the last decade, we have evolved our approach to auditing risk culture and behaviours – starting with a secondary "RCA" rating for our audit reports before establishing a specialist behavioural risk team.

Around four years ago, a shift began towards a more quantitative approach, employing empirical science techniques to test customer, colleague, and business outcomes. In doing so, we have tried to link how our processes, journeys, products or colleague behaviour impacts the decisions and outcomes of our customers.

While our size allows for specialist teams, there are elements that all teams can target. These include asking better questions about how an organisation's processes or behaviours impact customer outcomes (connecting culture to outcomes) and making greater use of data to test customer outcomes.

How have you cultivated a culture of innovation in your team?

Combining an experimentation mindset and practical application has been key. Teams construct a hypothesis and then gather data. The data is used to challenge the hypothesis, rather than validate it. The outcome and success of the experiment become information and learning about the hypothesis, regardless of whether the hypothesis is correct. This is important because the experiment is a success either way. Role-modelling and championing this attitude removes the fear of failure, creating psychological safety to try new things in a controlled way and celebrate the results.

This approach is actively promoted, and its outcomes are publicised within the function and has been highly effective.

Three key takeaways for functions of all shapes and sizes.

1. Independent assurance remains fundamental - it's our licence to operate.
2. Internal audit functions should increasingly use data, technology and AI to speed things up and reduce manual activity. We'll use data to focus our time on the biggest risks for our firms.
3. Internal audit should challenge themselves to move to a more forward-looking engagement model, proactively highlighting areas for improvement for their firms.

Banking and capital markets

Payments and financial crime

Updates on PSD3/PSR1 and the National Payments Vision

The Payment Services Directive 3 (PSD3), Payment Services Regulations 1 (PSR1) and the National Payments Vision (NPV) will drive the transformation of payments and digital assets in the EU and UK. The Financial Conduct Authority (FCA) issued a Dear CEO letter in February 2025 outlining priorities for firms, emphasising the importance of competition, innovation, and financial system integrity, and conducted a multi-firm review of risk framework and wind-down planning arrangements in Payment and E-Money firms (the "multi-firm review).

Five things you should know about the topic:

- **New EU regulatory structures under PSR1/PSD3:** The EU is shifting key definitions and conduct rules for payment institutions (PIs) from PSD2 to PSR1, while PSD3 retains oversight of PI authorisation and supervision. The EU also proposes to repeal the current E-money Directive (EMD), making e-money institutions (EMIs) a sub-category of PIs and merging EMI requirements into PSR1/PSD3. This will create regulatory divergence where firms operate in both the EU and UK, requiring adaptation of their compliance processes.
- **Expected deadlines for PSR1/PSD3 implementation and its impact:** The final PSD3/PSR1 ruleset is now expected late 2025, followed by an 18-month transition period with a 2027 go-live date. The impact will require careful consideration: new entities will come into scope, and major changes will be made to open banking services, re-licensing requirements, strong customer authentication (SCA) , additional information requirements and the opening of access to payment systems for non-banks.
- **The UK NPV:** Driven by the New Payment Vision Delivery Committee (NPDVC) and public-private collaboration, the UK's NPV aims to modernise the nation's payments infrastructure. Key initiatives in the NPV include upgrading the retail payments architecture, enhancing open banking, developing digital identity frameworks, exploring Central bank digital currency (CBDC) and stablecoins, and strengthening security and fraud measures.
- **FCA multi-firm review:** The FCA highlighted that, 'None of the firms we reviewed fully met our expectations, and in particular were not following the guidance in FG20/1.' Beyond the comprehensive expectations of FG20/1, firms should prioritise enterprise-wide and liquidity risk management frameworks, and consider group risk and wind-down plan arrangements.
- **Internal audit target operating model for new entrants:** Given the UK's focus on growth and innovation, new regulated firms require a robust three lines of defence model, including a highly effective internal audit function. The FCA expects strong internal controls, including operational resilience, financial crime controls, oversight of outsourced functions, and business continuity plans. Boards and regulators will scrutinise internal audit's coverage and target operating model.

Four things internal audit should do

1. **Assess strategic opportunity and business readiness (PSD3/PSR1)**

   Internal audit should assess the strategic and long-term business impact and related risks of proposed developments, including any additional regulatory or compliance requirements. For example, non-bank payment firms gaining direct access to payment systems represents a major change that increases compliance needs.

   Given the broad impact of new EU regulations, internal audit functions should determine whether robust readiness planning is in place to ensure compliance. Re-licensing under the new regime will require effective risk management, governance, and controls.

2. **Understanding upcoming impacts of the UK's NPV**

   Internal audit should understand how the business is monitoring and responding to the key developments set out in the NPV, including infrastructure upgrades and the payments forward plan. Regarding the NPV's focus on regulating stablecoins and other crypto-assets, internal audit should assess planned enhancements to the risk management and control framework.

3. **Evaluate changes to strong customer authentication**

   In the NPV, the government reconfirmed plans to revoke the SCA regulations embedded in the PSR 2017. This will allow the FCA to adopt more flexible, outcomes-based SCA rules designed to strengthen fraud prevention without imposing undue burdens on users. Industry engagement will continue in 2025.Internal audit should keep abreast of these changes and understand whether the impact of SCA changes can be addressed across their organisation.

4. **Assess internal audit coverage of risk management framework and wind down planning**

   Internal audit should consider reviewing risk management frameworks and wind-down plans to challenge and assess how management have incorporated the thematic review's findings.

   For internal audit functions in firms that have been subject to the FCA's thematic review, internal audit should review and challenge the design and effectiveness of management's remediation of regulatory findings.

Payments and financial crime

Changes to the safeguarding regime

In August 2025, the Financial Conduct Authority (FCA) released the Policy Statement PS25/12 on changes to the safeguarding regime for payment services and e-money firms. The publication includes final rules and guidance for the Supplementary Regime, which will become effective on 7th May 2026 after an implementation period of 9 months.

The Supplementary Regime will consist of: a) the applicable safeguarding regulations from the Electronic Money Regulations (EMR) 2011/Payment Services Regulations (PSR) 2017; b) the new Client Assets Sourcebook (CASS) Chapters 10A and 15 in the FCA Handbook; and c) the (amended) Chapter 10 of the FCA's "Payment Services and Electronic Money – Our Approach" document.

The FCA may make further changes to the safeguarding regime once the EMRs and PSRs are repealed under the Financial Services and Markets Act 2023, as planned by His Majesty's Treasury.

Five things you should know about the topic:

- **Why the FCA is updating the safeguarding regime**: following several high-profile firm failures, many of the customers seeking to recover their funds faced prolonged delays and shortfalls in the amounts ultimately returned. The new rules aim to raise standards in the sector by removing ambiguities in certain areas of practice.
- **Understanding the transaction flows that impact customer funds will be more important than ever**: the new rules and guidance include updates to some of the ways in which the legal definitions of relevant funds apply when scoping the safeguarding obligation. A clear analysis of the fund flow is therefore essential to justify the policy decisions that drive the safeguarding methodology.
- **The expectations for reconciliations will now be codified in the rulebook**: the FCA is clarifying its expectation that firms must perform internal reconciliations as well as external reconciliations. The regulator has set out unambiguously that it will require firms to perform mandatory reconciliations at least once each reconciliation day (which excludes weekends, bank holidays and days on which relevant foreign markets are closed).
- **New areas of safeguarding practice**: the FCA is introducing CASS Chapter 10A requiring safeguarding institutions to maintain a mandatory "CASS Resolution Pack" and submitting monthly "Safeguarding returns" to the FCA, similar to the existing CASS Client Money and Asset Returns ("CMARs").
- **There will be greater scrutiny around Safeguarding audits**: annual reports will be mandated. They will require an auditor that is eligible under the Companies Act 2006 and will need to follow a specific standard (with relevant guidance expected to be published by the Financial Reporting Council (FRC)). The auditors will submit their reports directly to the FCA.

Three things internal audit should do

1. **Risk based internal audit coverage over safeguarding controls.**

   As a point of reference, the current Financial Reporting Council (FRC) Client Assets Standard specifies that the independent external CASS auditor should evaluate the role of the IA function in the context of the firm's system of internal control over CASS arrangements.

   The FCA intends for a similar FRC audit standard to that of CASS arrangements to be produced for safeguarding, which is likely to include equivalent expectations for such an assessment. This implies that internal audit performs a different important assurance role to both that of the statutory external auditor, and the external independent auditor that has completed the required annual reasonable assurance safeguarding audit.

   In addition, the Dear CEO Letter issued to payments firms in February 2025 re-iterates several areas firms should act on. This included safeguarding, placing the emphasis on how the three lines of defence model should ensure compliance and keep customer money safe.

2. **Assurance over interim and end state rules readiness.**

   Internal audit should consider reviewing whether controls are adequately designed (and effectively embedded) in readiness for the newly implemented safeguarding regime.

3. **Deep dives over key processes in your business model that drive compliance.**

   Under the proposed future safeguarding regulatory requirements, certain topics such as the new CASS Resolution Pack and regulatory reporting will be out of scope of the external safeguarding audit. Further areas of practice that are fundamental in driving the approach to compliance, such as the assumptions that have been made in determining relevant funds, should also be assessed for coverage.

   Where key issues have been raised as part of the external audit or the safeguarding audit, internal audit can add value by providing assurance over the validation of actions implemented to ensure findings are remediated in a timely way.

Prudential and credit risk

Credit risk

The onset of 2025 has been marked by a surge in uncertainty for the UK economy. Concerns about cost-of-living pressures are easing. However, geopolitical risk and sector specific challenges have replaced inflation and interest rate worries. Firms must maintain agile and robust governance, controls, and reporting frameworks to accurately reflect emerging risks, including effective credit risk models and proactively identifying and monitoring vulnerable portfolio segments.

Four things you should know about the topic:

- **Economic uncertainty – identification and response to novel and rapidly evolving risks**: An unpredictable geopolitical and economic climate requires a reassessment of sector-specific and counterparty risks. As the Prudential Regulatory Authority (PRA) and European Central Bank (ECB) have stressed, robust credit risk management frameworks, and incorporating forward-looking scenarios that account for these uncertainties, are important for identifying vulnerabilities and informing strategic business planning.
- **Model design and calibration**: The credit modelling landscape offers opportunities despite its challenges. Post-pandemic data enables model recalibration, addressing outdated assumptions, especially crucial for loss given default models. Internal Ratings Based (IRB) firms must also adapt their downstream models to regulatory capital model changes. Industry practice continues to evolve on IFRS9 SICR calibration. PRA maintain their emphasis on consistent application of IFRS 9 staging, highlighting the inadequacy of current subjective practices.
- **Credit risk governance**: Sound credit risk governance is vital in today's volatile credit landscape, including identifying vulnerable sectors, defining risk appetite, validating innovative complex AI/ML models, and effectively using management judgements to capture unmodelled risks – a key ECB focus. Governance frameworks often lack a forward-looking perspective, hindering identification of emerging risks, particularly for smaller firms facing data limitations and model monitoring challenges.
- **Effective use, control and reporting of data**: High-quality data is crucial for credit risk modelling, yet weaknesses persist in data aggregation and risk reporting, getting continued supervisory attention. Rapid technological advances are not lessening, exposing firms to data risks, and to keep pace, digitalisation remains an essential element of risk management. Senior leadership must be proactive in embedding robust control frameworks, aligned with standards like BCBS 239, and ensure management information is accurate, concise, timely, relevant, actionable, and highlights emerging risks to support effective decision-making.

Five things internal audit should do

1. **Economic uncertainty: identification and response to novel and rapidly evolving risks**

   Internal audit should assess existing frameworks to ensure robustness and adaptability, and ensure firms possess a strong understanding of their portfolio's exposure to geopolitical risks, exploring stress testing and scenario analysis to evaluate the likely impacts. The extent of their exposure to country risk must also be considered.

2. **Model design and calibration**

   Internal audit must verify the robustness of credit models, analysing underlying assumptions against current data and assessing downstream model resilience to upstream regulatory changes. Model monitoring and IFRS9 SICR calibration frameworks should be considered for targeted review.

3. **Credit risk governance**

   Internal audit functions should assess the effectiveness of credit risk management frameworks in identifying and tracking emerging risks. This includes reviewing risk appetite, policies, model validation, governance, accountabilities, and committee responsibilities. A targeted review should scrutinise oversight of management judgements and model overlays.

   Internal audit's credit risk plan should incorporate collaboration with the second line of defence, whilst also considering any remediation items arising from external credit risk audit reviews.

4. **Effective use, control and reporting of data**

   Internal audit should assess credit risk model data controls for BCBS 239 compliance across the entire data lifecycle. This includes robust testing, a scalable control framework, and scrutiny of management information used for key committee decisions. Emerging data risks from technology advancements should be considered.

5. **Intelligent risk assessment**

   Internal audit should innovate and evolve their risk assessment approach. Focus should be on transforming risk assessment leveraging data-driven insights and leading-edge analytical tools. This reduces manual effort, enhances risk detection, and drives greater efficiency.

Prudential and credit risk

Prudential risk

As UK banks and building societies develop their internal audit plans for the upcoming year, the regulatory environment continues to evolve with respect to prudential risk, presenting both challenges and opportunities. The Prudential Regulation Authority (PRA) is simultaneously implementing several reforms to capital and liquidity frameworks for smaller and larger firms, alongside a significant change to building society regulation. Internal audit functions should review the near-final rules, as well as the rules and guidance in consultation, to understand the impact on their respective firms, and the appropriateness of management's plans to comply.

Five things you should know about the topic:

- **PRA CP12/25 & Pillar 2A methodologies:** Internal audit needs to understand the PRA's proposed changes to Pillar 2A methodologies, which refine assessments of individual capital needs beyond Pillar 1, impacting areas like credit and operational risk.
- **Embedding Basel 3.1:** Implementation demands continued audit focus. This impacts credit, market, and operational risk, plus introduces an output floor, necessitating significant system and data upgrades, even in light of the delays to some elements of the Basel 3.1 as announced by the government in July 2025.
- **Small Domestic Deposit Taker (SDDT) regime:** For firms opting into the SDDT regime, internal audit must ensure effective transition and ongoing compliance with its proportionate prudential requirements.
- **Regulatory reporting:** The PRA's 2025 banking priorities letter has highlighted the risk of having quality and unreliable data which feeds regulatory calculations and reporting. The PRA have signalled their intention to review data accuracy utilising a full range of supervisory tools.
- **Removal of SS20/15 (building societies only):** The proposed withdrawal of SS20/15 gives building societies more flexibility in treasury and lending risk management, but requires them to demonstrate robust risk management frameworks aligned to any new lending or treasury activity.

Five things internal audit should do

1. **Pillar 2a methodologies**

   Provide assurance over management's interpretation of new rules and guidance, and overall readiness for these changes, focusing on the assumptions for new calculation methodologies, (such as the introduction of scenario analysis for Pillar 2A credit risk), and the integration of these changes into the ICAAP. Verify the accuracy of associated regulatory reporting.

2. **Basel 3.1**

   Periodic reviews of management's plan and glidepath to go-live for Basel 3.1. Analyse management's interpretation of the updated standardised approach to credit risk. Verify data and systems readiness and ensure preparedness for revised regulatory reporting.

3. **SDDT Regime**

   Review the firm's eligibility for specific aspects of the SDDT regime, e.g. compliance with Retail Deposit Ratio to disapply Net Stable Funding Ratio requirements. Evaluate the firm's initial simplified ILAAP document against new requirements. Assess the appropriateness of the risk management framework under this regime.

4. **Regulatory reporting**

   Review the firm's end-to-end regulatory reporting process, identifying control gaps which may contribute to inaccurate and unreliable data being used in reporting, considering the PRA's 2025 banking priorities letter. Review control around data flow from legacy systems and manual data inputs, as well as plans to move to more reliable automated solutions.

5. **Removal of SS20/15 (building societies only)**

   Evaluate how the society is adapting its treasury and lending risk frameworks. Assess management and board oversight of these revised strategies whilst opining on the skills and experience required to effectively manage new risks across all lines of defence and at Board level. Review controls around treasury operations (ensuring derivative use is for hedging) and examine lending policies for continued prudence. Ensure the ICAAP and ILAAP reflect these changes.

Conduct risk

Mortgage rule simplification

The Financial Conduct Authority's (FCA) SP25/11, sets out targeted reforms to mortgage regulation, aiming to simplify the existing framework while preserving consumer protection through the Consumer Duty. Key changes include increased flexibility for execution-only mortgage sales, streamlined affordability assessments for mortgage term reductions and remortgaging, and retiring outdated non-handbook guidance. The policy statement seeks to balance consumer choice, competition, market flexibility, and responsible lending while embedding outcomes-focused supervision.

Five things you should know about the topic:

- **Execution-only sales flexibility:** The FCA has enabled the removal of the automatic advice trigger during customer interactions, allowing more consumers to transact on an execution-only basis while requiring firms to identify vulnerable customers needing advice.
- **Mortgage term reductions simplified:** Firms will no longer be required to conduct full affordability assessments for term reductions, provided it's in the best interests of the borrowers, plus where the borrowers are not increasing their loan amount and are up to date with payments.
- **Modified affordability for remortgaging:** Firms can expand Modified Affordability Assessments (MAA) to allow external remortgaging if deals are cheaper than existing terms or equivalent offers from their current lender, promoting competition.
- **Retirement of non-handbook guidance:** Existing guidance (e.g. FG13/7) on dealing fairly with interest-only mortgage customers has been retired, with Consumer Duty acting as the primary framework for ensuring appropriate customer outcomes. Whilst Mortgage Conduct of Business (MCOB) requirements already in place do require a review of the customer's repayment strategy for their interest-only mortgage during the term, firms will need to evidence that customer needs and vulnerability factors are considered, foreseeable harms are identified, and good outcomes are being delivered throughout the mortgage term.
- **Increased risk-based responsibility for firms:** While the new policy statement offers flexibility, it increases reliance on firm governance, policies, and processes to ensure risks such as customer harm, product suitability, and affordability are effectively managed. Increased use of flexibility will depend on individual risk appetite and means those willing to engage, will likely be accepting more risk (for example, using a simpler assessment of a customer's ability to afford future monthly payments). These reduced prescriptive FCA rules, puts the onus on firms to actively manage risks of customer harm, product suitability, affordability, and vulnerability through their own frameworks. Firms will need clear governance and oversight arrangements, outcome-focused management information (MI), well-documented decision-making and strong third line challenge.

Three things internal audit should do:

1. **Readiness and post-implementation review**

   Internal audit should assess readiness for go-live and provide assurance over the programme governance structure in place to oversee implementation of the rule changes and changes to the control framework, including appropriate Board and senior management oversight.

   Conduct post-implementation reviews to confirm whether changes have been embedded effectively with appropriate ongoing monitoring in place through robust management information. Evaluate how customer outcomes are being tracked and monitored post-implementation.

2. **Updated responsible lending policy and associated procedures**

   Evaluate revised responsible lending policy, associated procedures and affordability assessment models for term reductions and remortgaging (through a MAA) to assess that they are compliant with requirements, performing as expected and changes are delivering good outcomes for customers. This could include sample reperformance of underwriting assessments to assess alignment to new processes and whether the firm has delivered a good outcome for the customer, including design and operating effectiveness of controls.

3. **Execution-only sales journey controls**

   Assess whether execution-only processes are functioning as intended — including testing customer journeys to confirm that disclosures are provided at the right points, that customers fully understand the implications of proceeding without advice, and that controls are in place to identify cases where advice should still be recommended (i.e. customers whose main purpose is debt consolidation).

Conduct risk

A focus on consumers – Motor finance and BNPL

After a year of uncertainty, the Financial Conduct Authority (FCA) has offered clarity on motor finance redress after announcing it will consult on an industry-wide redress. Simultaneously, the countdown to Buy Now Pay Later (BNPL) regulation is on. The Treasury's consultation response confirms the FCA's upcoming oversight of BNPL, leaving firms to anticipate detailed rules within the next year – regulation day is 15 July 2026. This dual regulatory shake-up demands proactive adaptation from financial institutions.

The consumer impact is substantial: as of 2025, two in five UK adults (42%) have used BNPL services at some point, amounting to approximately 22.6 million people. This is an increase of 36% at the start of 2023. Millions are expected to be impacted by the motor finance redress - the FCA estimates that firms may need to pay out up to £18bn.

Five things you should know about the topic:

Motor finance

- **An industry-wide scheme announced:** The FCA announced that it will consult on a redress scheme with a six-week consultation expected in October 2025. The FCA estimates that this could cost affected firms up to £18bn.
- **Preparing for the redress scheme:** The FCA has not yet provided any indication on what the parameters of such a redress scheme would include, for example, whether the scheme itself would be voluntary or involuntary, be run on an opt-in or opt-out basis, whether it would be sanctioned under s404 of the Financial Services Act or as part of a scheme of arrangement. While prior schemes sanctioned by the FCA may not be directly comparable, the read-across that can be applied from these prior schemes does indicate some no-regret actions that firms should consider now to sufficiently prepare both operationally and financially for this type of remediation activity.
- **Our latest regulatory view** on this can be found at Motor Finance Commission Arrangements – Time to Act? | Deloitte UK

Buy Now Pay Later

- **15 July 2026 – regulation day:** Between the FCA's consultation and "Regulation Day", BNPL firms will have a short time window to evaluate how the new BNPL regime will impact their business models and determine if authorisation is required. Irrespective of whether authorisation is required, firms will need to prepare to ensure that they have robust processes, systems, frameworks, and resources in place to support regulatory compliance and to evidence the delivery of good customer outcomes.
- **Our latest thinking** can be found at Countdown to Regulation Day for Buy-now-pay-later (BNPL) firms | Deloitte UK

Three things internal audit should do:

1. **Challenge the robustness of project plans**

   Once the regulator announces final regulatory requirements for both key areas of focus, internal audit functions should critically assess the comprehensiveness of plans drawn up by management to ensure that they are designed to meet regulatory requirements in line with the required timescales.

2. **Design a programme of assurance**

   Internal audit functions should ensure that regular assurance is provided to those charged with governance. A robust programme of assurance should be implemented following issuance of the regulations with updates to those charged with governance at appropriate intervals.

   Integrated assurance across the three lines of defence will be imperative.

3. **The BNPL journey**

   Existing firm processes will likely require redevelopment or refinement to meet evolving regulatory demands. Key areas requiring attention include financial promotions, creditworthiness assessments, disclosures, servicing, and complaint handling.

   Internal audit should be proactive in understanding the plans of the business to identify necessary new controls and adapt existing frameworks to ensure full compliance with the Consumer Duty regulations, which impact all stages of the customer lifecycle.

Sector deep dive

Global markets

With many policymakers focused on economic growth and removing regulatory barriers to achieve it, there is cause for cautious optimism within global markets, despite heightened geopolitical volatility. However, firms face a sizeable package of implementation effort (including CRD VI, SS5/21, T+1 settlement transition) and will need to optimise and prioritise for success.

Five things you should know about the topic:

- **Settlement transition to T+1**: The UK and the EU have committed to implement the securities settlement transition to T+1 on 11 October 2027 and align as much as possible in the process. Firms need to plan and budget now for an extensive multi-year transformation to meet the deadline.
- **Capital Requirements Directive VI (CRD VI) is now law:** Firms with third country banking branches in the EU and non-EU firms that provide certain banking products to EU clients must start their planning now. Firms need to move beyond an initial assessment and towards a defined strategy for servicing EU clients in order to allow time for legal entity changes, staffing adjustments, regulatory applications and smooth client transitions before 11 January 2027.
- **Booking model arrangement**: The Prudential Regulation Authority (PRA) has finalised its approach to branch and subsidiary supervision (SS5/21). It has clarified the scope of application of booking model arrangement expectations, provided some further guidance on the materiality of booking model changes, and clarified its expectations for remote booking, consolidated risk management oversight of split desks and trader controls. The new policy took effect immediately on publication (20 May 2025); all in-scope firms need to complete a self-assessment against the PRA's revised expectations and agree with their supervisor a timeline for any required remediation.
- **Counterparty credit risk**: There continues to be an increased regulatory focus on counterparty credit risk following high-profile defaults, and the liability driven investment (LDI) crisis. Areas of regulatory focus include firms' choice of metrics to measure stressed counterparty credit risk (CCR) exposure, due diligence and client onboarding controls, watchlist processes, and identification of illiquid, concentrated or hard-to-replace positions.
- **Transaction reporting**: The Financial Conduct Authority's (FCA) Market Watch 82 highlighted persistent inefficiencies in transaction reporting, which suggest some firms need to improve their operational frameworks. Observations covered remedial timelines, back reporting, and transaction reporting errors and omissions notifications (i.e. breach notifications).

Five things internal audit should do

1. **T+1 settlement transition**

   Review the firm's T+1 settlement transition plan, including programme governance, focusing on the work being performed by the business to ensure all parties in the settlement chain are prepared for the transition (e.g. client engagement and education).

   Review of the lessons learned from the US implementation and how they can be applied to the UK/EU firm.

   Perform readiness testing and reporting to those charged with governance, including integrated technology reviews.

2. **CRD VI**

   Review the firm's CRD VI impact assessment, and its coverage of entities, products, services, and client relationships.

   Provide transformation/change assurance, including an assessment of the firm's CRD VI implementation programme, focusing on higher impact workstreams such as strategy and front office, legal, and governance.

3. **SS5/21**

   Firms will need to provide the PRA with a clear explanation of any gaps against the policy and proposed timeframe to address them. Internal audit should review this information and monitor the completion of actions against agreed timelines, as well as review internal self-assessment results and remediation plans.

4. **Counterparty credit risk (CCR)**

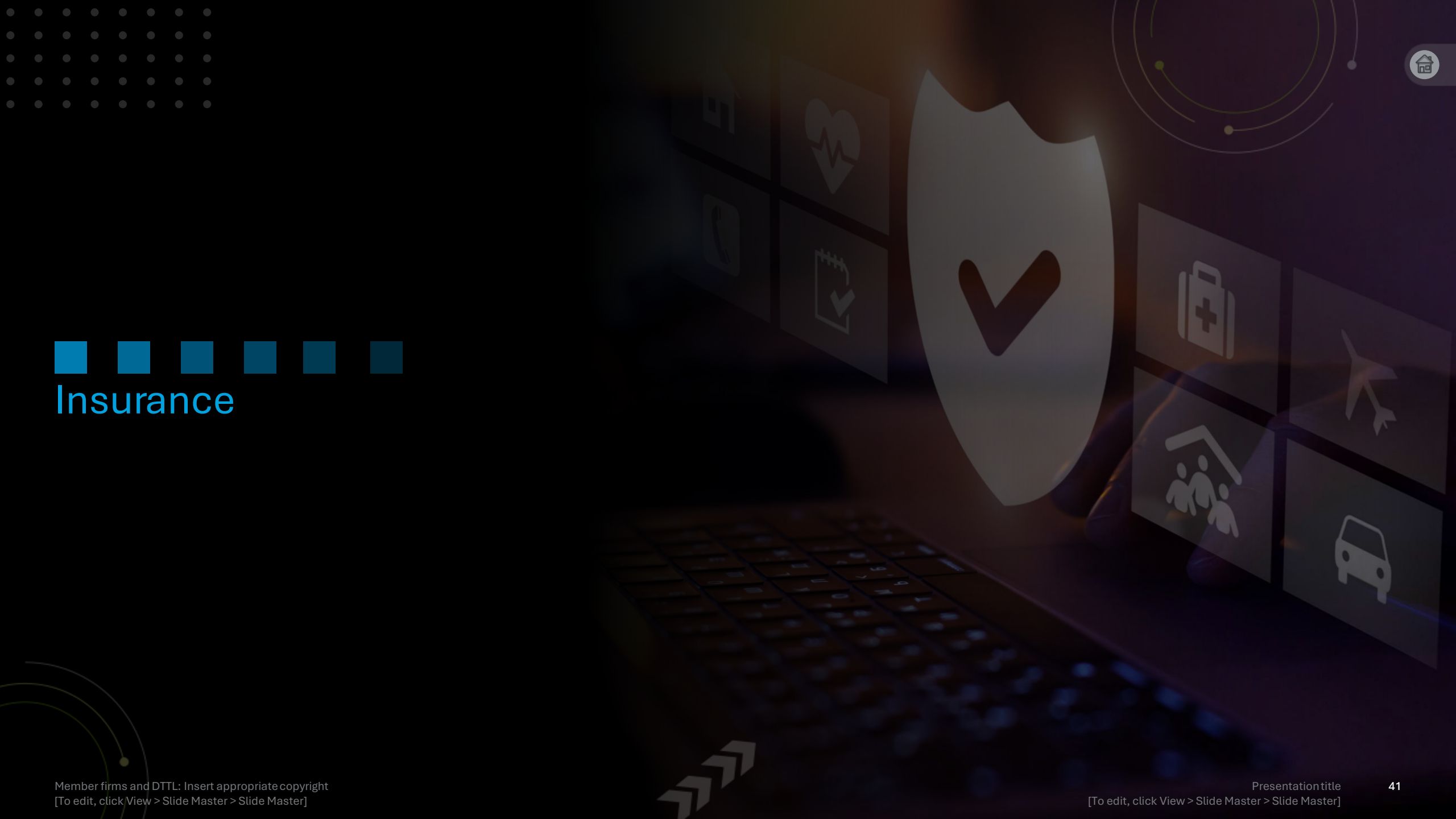
   While reviewing the firm's risk management framework and controls, include coverage of CCR calculations and their impact on overall risk management strategy.

   Assessment of data quality and alignment with regulatory rules, including the use of analytics techniques.

5. **Transaction reporting**

   Internal audit should be involved in the testing of remedial actions taken to address regulatory issues. This should include coverage of errors, back reporting and omissions notifications.

Insurance



Conduct risk

General insurance and premium finance

The Financial Conduct Authority (FCA) has published four significant reviews of general insurance (GI) retail practices, accompanied by a roadmap outlining next steps. These reviews covered motor insurance claims, claims handling (home and travel), premium finance, and General Insurance Pricing Practices (GIPP). The findings highlight areas for improvement, particularly in claims handling and premium finance, where the FCA indicated potential supervisory interventions.

Five things you should know about the topic:

- **Targeted interventions:** While the reviews are extensive, the FCA's immediate focus is on home, travel, and premium finance. Firms should expect individual follow-up on claims handling concerns.
- **Premium finance concerns:** Annual Percentage Rates (APR) exceeding 30% being charged to 20% of premium finance customers raise concerns about fair value and suitability. Firms should proactively review their practices in anticipation of the final report in late 2025.
- **Motor insurance claims costs:** Rising claims costs, largely outside firms' control, are driving premium increases. However, the FCA is scrutinising outsourcing practices and referral fees that may inflate costs and negatively impact customer outcomes.
- **Claims handling deficiencies:** The FCA identified weaknesses in claims handling processes, particularly in outsourcing arrangements, management information (MI), and governance. Specific concerns include travel insurance service failures and customer understanding of home insurance policies.
- **GIPP compliance:** While GIPP compliance is generally satisfactory, the FCA acknowledges the associated costs and administrative burden. Further regulatory data reporting requirements are under consideration.

Five things internal audit should do

1. **Claims handling review**

   Assess the firm's claims handling processes, focusing on outsourcing arrangements, MI quality, and governance. Identify and address any gaps in compliance with FCA expectations, particularly concerning home and travel insurance.

2. **Premium finance review**

   Review the fair value and suitability of premium finance products, paying close attention to APRs and customer outcomes. Assess compliance with all relevant regulations and best practices.

3. **Motor insurance claims cost analysis**

   Investigate the firm's outsourcing and referral fee arrangements within the motor insurance claims process. Assess the impact on claims costs and customer outcomes.

4. **GIPP compliance review**

   Review compliance with GIPP principles, considering the associated costs and administrative burden. Assess the firm's readiness for potential changes in regulatory data reporting requirements.

5. **FCA roadmap implementation**

   Develop a plan to address the FCA's recommendations and next steps outlined in the roadmap, including the review of motor insurance costs for various customer groups and the preparation for the final premium finance report.

Conduct risk

Price and value outcomes

Products and services must deliver fair value to customers. The Financial Conduct Authority's (FCA), through its updated product oversight and governance sourcebook (PROD) (chapters 4.2 and 4.3), now places increased regulatory pressure on insurers and distributors to ensure that their offerings consistently meet customer needs and expectations.

The FCA has issued numerous regulatory communications in the last couple of years aimed at firms demonstrating much greater rigor in how they assess, evidence and oversee fair value across the entire product cycle. It is evident that firms must now take these lessons learned, and if they have not yet done so, commit to making enhancements to their price and value frameworks.

Three things you should know about the topic:

The FCA strengthened the requirement for firms to ensure that insurance products and services provide fair value to customers in 2021. In August 2024, the FCA published the results of its thematic review commenting whether firms were meeting their product governance obligations for general insurance and pure protection products under these new rules. Price and value continue to be the subject of FCA regulatory intervention in 2025 with firms being directed to make enhancements to their frameworks and management information. As a result of the FCA findings, we have identified three key focus areas to help firms deliver good customer outcomes:

- **Price and value framework:** Insurers need to re-design their price and value frameworks, underpinned by metrics and data across six key pillars: product design, features and benefits, total price, remuneration/commission, customer utility, quality of service, and distributor value. Equally, distributors need to have in place their own price and value frameworks for their services, collecting data on the distribution strategy and target market, remuneration they receive, and customer utility of their services.
- **Customer groups:** Data should be collected on different customer groups, including vulnerable customers, to understand their end-to-end journey experience (including claims), and to assess whether all customer groups are in receipt of good customer outcomes.
- **Monitoring and evaluation:** Firms should have in place governance and oversight of the results of price and value assessments, with accurate and timely management information to help senior management make informed decisions.

The shift reflects FCA's ongoing Consumer Duty drive – pushing firms to go beyond box-ticking and embed meaningful, customer centric oversight into their operations.

Three things internal audit should do:

1. **Price and value framework**

   Assess whether there is a documented framework and methodology which are aligned to PROD 4.2 (insurers) and PROD 4.3 (distributors), understand the key metrics and ability to understand outcomes for different customer groups, accuracy of data and associated tolerances with an appropriate rationale.

   This will include value of specific features, benefits and add-ons for insurers, and the commission arrangements for distributors.

2. **Customer groups**

   Assess whether there is sufficient granularity in the price and value assessments to consider different customer groups, and that timely and accurate MI is available to perform assessments.

   Testing should include a review of a sample of assessments, assessing the processes and controls used to reach judgements, with evidence that actions are performed in a timely manner.

3. **Monitoring and evaluation**

   Assess whether there is effective governance and oversight of price and value assessments, including timeliness and availability of data and quality of commentary to verify whether there is sufficient oversight of vulnerable customer outcomes. In addition, consider whether the reporting on product reviews, price and value assessments are sufficiently granular to consider outcomes for vulnerable customer groups within a product(s) target market.

Investment and wealth management

Prudential and credit risk

Internal capital and risk assessment (ICARA)

The Financial Conduct Authority (FCA) continues to review and provide feedback on prudential arrangements at investment firms. Most recently, the FCA published observations (March 2025) following a review of liquidity risk management at wholesale trading firms. In addition, the FCA's previously published ICARA observations continue to be relevant and cover some key areas that firms should be considering, including liquidity, wind-down planning and risk appetite.

As firms have now had their ICARAs in place for three years, the priority for many is shifting from the design to the operability of the process. This includes, for example, ensuring efficient and effective linkage and consistency between the ICARA and other relevant processes, operational resilience and third-party risk management.

Five things you should know about the topic:

- **FCA liquidity risk review:** The FCA recently conducted a review of liquidity risk management at wholesale trading firms and released some detailed feedback on their observations, including providing examples of good and poor practice. Although their review focused on trading firms, some of the principles and good practice can be applied to other firms subject to ICARA.
- **Wind-down plan testing:** Wind-down plans continue to be an area of focus for the FCA and as firms make enhancements to the design of their wind-down plans, the focus is shifting to operability of wind-down arrangements. The FCA has indicated that testing of wind-down plans is considered to be good practice, for example using fire-drills and simulations.
- **The role of KRIs and risk frameworks:** Across investment firms, risk frameworks range in maturity. Regardless of the maturity of the framework, developing effective KRIs and early warning indicators is essential for effective and proactive management of risks and the effective design of risk appetite frameworks can be an important tool in the management and prevention of harm. Well-designed frameworks and MI/KRIs help Boards oversee the risk profile of the organisation more effectively.
- **ICARA and outsourcing:** As the volume, criticality and complexity of outsourcing arrangements increases, it is important to fully assess the management and controls within the framework, including under stressed conditions for ICARA purposes. This will enable more accurate assessment of both the financial as well as non-financial resources required under the ICARA.
- **Minimising model risk:** Investment firms use a range of standard and non-standard models in their prudential calculations, assessment and mitigation of risk. There is an on-going expectation on Boards and senior management to ensure adequate understanding, oversight, challenge and application of these key processes. Both standard and non-standard models should also be reviewed and validated to minimise the risk of errors impacting the resulting output and/or key decision-making processes.

Five things internal audit should do

1. **Liquidity risk framework**

   Internal audit should assess whether the liquidity risk framework remains fit for purpose, reviewing the design and effectiveness relative to the activities of the firm. This should take into consideration the FCA's feedback in Q1 2025.

2. **Wind-down plan testing**

   Wind-down plan testing can help to identify areas where the plan can be strengthened to make it more operable. A key area of focus should be governance, as a strong and well-designed governance framework can help to ensure quick and effective decisions are made to reduce harm (including to customers and markets).

3. **Risk appetite framework**

   Internal audit functions should check the effectiveness of the risk appetite framework. This would include whether early warning indicators are effective and set at the right levels. The FCA has indicated that firms should consider stress impacts when identifying internal points of intervention.

4. **Linkage between difference processes**

   Internal audit teams should undertake a process assessment as part of their overall review, checking the consistency of conclusions across different arrangements e.g. ICARA and wind-down assessment, operational resilience and third-party risk management framework.

5. **Prudential model validation**

   Internal audit can ensure models used in prudential calculations is considered as part of model risk framework internal audit scope. Non-standard models should also be reviewed as issues in such models can lead to outputs being significantly impacted.

Sector deep dive

Pensions

The UK pensions landscape is continuously transforming. Pensions reform focusses on utilising pension scheme assets to invest in the UK, and the implementation of the own risk assessments (ORAs) represents an increased focus on proactive risk identification and mitigation across pension schemes, whilst pension dashboards are improving transparency by giving individuals a single, consolidated view of their pension savings. Pension scheme consolidation offers cost savings and improved governance, and automation is streamlining administration, boosting efficiency and accuracy. These changes present both challenges and opportunities, demanding better data management, robust risk oversight, and adaptable administrative practices.

Five things you should know about the topic:

- **ORA deep dive:** Effective 2026, the ORA will be integral to a scheme's comprehensive risk management strategy, moving beyond mere compliance. This requires proactive identification of emerging risks, such as climate change and cybersecurity, and continuous monitoring to adapt to evolving circumstances. The Pensions Regulator (TPR) and internal audit will rigorously scrutinise the ORA's quality and thoroughness.
- **Pension dashboards impact:** The 2026 rollout of pension dashboards necessitates schemes ensuring accurate, accessible, and compliant data. This requires robust data management including the validity of data, particularly for deferred members. Non-compliance risks, reputational damage and regulatory action.
- **Scheme consolidation:** Driven by cost reduction, improved governance, and economies of scale, pension scheme consolidation is accelerating. This involves transferring assets and liabilities from smaller schemes into larger, more robust ones. Successful consolidation demands thorough due diligence, robust legal frameworks, and efficient administration to ensure smooth transfers and minimise member disruption.
- **Automation's expanding role:** Automation is revolutionising pensions administration, streamlining tasks like data entry, reconciliation, and reporting to improve efficiency, reduce costs, and enhance accuracy. Successful implementation needs careful planning, appropriate technology choices, and robust change management.
- **Cybersecurity remains paramount:** The digitalisation of pensions administration increases the risk of cyberattacks. Schemes must invest in strong security measures, including controls, regular audits, and employee training, to protect sensitive member data and mitigate cyberattack risks.

Five things internal audit should do

1. **Enhanced ORA audit**

   A comprehensive internal audit of the ORA should be undertaken, not just assessing its completeness, but also its effectiveness in identifying and mitigating risks. This includes reviewing the accuracy of risk assessments, the adequacy of control designs, and the effectiveness of control operation.

2. **Assess skills and resources**

   Internal audit functions must ensure they possess the necessary expertise and resources to provide assurance across the full spectrum of pension scheme risks including funding and liquidity, operational resilience and value for members. This may involve upskilling existing staff or engaging specialist external consultants. They also need to conduct a thorough review of independence within the internal audit process.

3. **Revised investment strategies**

   As schemes look to meet the requirements of pensions reform, they may need to revisit the statement of investment principles, transition assets and invest in new asset classes. Where this is the case, appropriate controls should be in place to monitor risks and performance ensuring alignment with the investment objectives.

4. **Robust Third-Party Assurance**

   The processes and controls implemented by schemes to identify, onboard, monitor and exit third-party service providers should be subject to internal audit with specific focus around service level adherence, data management and business continuity capabilities.

5. **Focus on data integrity**

   With increasing reliance on data, including pension dashboards, internal audit should focus on the integrity and accuracy of pension scheme data throughout its lifecycle. This includes data entry, processing, storage, and reporting.

Sector deep dive

Investment management

The investment management sector has come under close attention from the regulator during the first half of 2025, with the Financial Conduct Authority (FCA) completing reviews into both private market asset valuations and ongoing financial advice services.

Private market investments continue to be an area of significant growth within the industry. With the increased level of judgement involved in these valuations, the FCA reviewed the robustness of firm's processes and governance in this area.

In line with its Consumer Duty priorities, the FCA maintains a sharp focus on value demonstration, especially regarding ongoing advice servicing provided by advisory firms. While not identifying systemic issues, the FCA's February 2025 observations highlighted the need for investment management firms to proactively ensure service delivery aligns with client agreements and expectations or face potential refund obligations.

Two things you should know about the topic:

- **Private market asset valuations:** Given the FCA's recent scrutiny of private market asset valuations, robust processes demonstrating independence, expertise, transparency, and consistency are essential. While some firms exhibited these strengths, the FCA's review identified areas for improvement, including consistent identification and documentation of conflicts of interest, ensuring sufficient independence within the valuation process itself, and establishing a consistent approach for ad-hoc valuations.
- **Ongoing financial advice services:** The FCA review highlighted both positive practices and areas requiring improvement. Firms demonstrating good practice clearly communicated the nature and timing of client reviews, implemented policies to cease charging fees where clients had not engaged with the service for a specified period, and diligently ensured that client circumstances, objectives, risk profiles, and capacity for loss were regularly updated. However, the review also revealed that in fewer than 2% of sampled cases, firms had not attempted to conduct an ongoing suitability review, a significant lapse that will likely necessitate remediation and potential redress. Firms should proactively assess their ongoing advice services to identify and remediate any instances where clients may have been disadvantaged.

Two things internal audit should do

1. **Private market valuations**

Internal audit should assess the robustness of the firm's governance arrangements for valuations. This includes reviewing the effectiveness of valuation committees, the detail and accuracy of record-keeping regarding valuation decisions, and the clarity of accountability for valuation processes.

Include focus on independence/conflicts of interest within audits of valuations. This includes conflicts related to fees (especially in open-ended funds), asset transfers, redemptions/subscriptions, investor marketing, secured borrowing, and potential uplifts/volatility adjustments.

Higher risk areas include ad hoc valuations which do not follow standard valuation methodologies.

2. **Ongoing financial advice services**

Internal audit should conduct a review of the firm's processes for delivering ongoing advice services, focusing on suitability reviews, with reference being made to the good practices and areas of concern highlighted by the FCA. This review should assess the completeness of suitability review offerings (utilising data analytics where possible), and the controls in place to ensure these reviews are offered where required.

Evaluate the adequacy of management information covering all aspects of ongoing advice servicing, including scheduled reviews, completed reviews, missed reviews, client complaints, and refund processes. Assess the firm's ability to identify trends, remediate issues, and provide meaningful reporting to senior management.

Key contacts - Australia

Financial Services Controls Assurance

James Oliver
Controls Assurance Partner
+61 (0) 3 9671 7969
joliver@deloitte.com.au

Renuka Vaiude
Controls Assurance Partner
+ 61 (0) 3 9671 6006
rvaiude@deloitte.com.au

ASX Listed Entities Control Assurance

David Boyd
Controls Assurance Partner
+ 61 (0) 3 9671 7077
davidjboyd@deloitte.com.au

Claire Hoy
Controls Assurance Partner
+61 (0) 7 3308 7273
clhoy@deloitte.com.au

Benoy Shankar
Controls Assurance Partner
+61 (0) 8 9365 7062
bshankar@deloitte.com.au

Key contacts and contributors

Geopolitical risk and regulatory streamlining

Mahmood Zaman
Director
mazaman@deloitte.co.uk

Vincent Greenaway
Senior Manager
vgreenaway@deloitte.co.uk

Zoya Baig
Senior Manager
zoyabaig@deloitte.co.uk

GenAI

Lewis Keating
Director
lkeating@deloitte.co.uk

Payments and safeguarding

Phil Ackroyd
Senior Manager
packroyd@deloitte.co.uk

Nikhil Kulkarni
Assistant Director
nkulkarni@deloitte.co.uk

Sukhjit Saundh
Associate Director
sssaundh@deloitte.co.uk

Steve Bailey
Director
sjbailey@deloitte.co.uk

Digital assets

Ed Moorby
Partner
emoorby@deloitte.co.uk

Fraud

Andrew Barnett
Director
ajbarnett@deloitte.co.uk

Melina Andreou
Manager
melinaandreou@deloitte.co.uk

Financial crime

Andrew Oates
Partner
aoates@deloitte.co.uk

Zeynep Ersoz
Director
zersoz@deloitte.co.uk

Credit risk

Richard Tedder
Partner
rtedder@deloitte.co.uk

Deepan Chakraborty
Associate Director
dchakraborty@deloitte.co.uk

Model risk management

Justin LeBlanc
Assistant Director
jusleblanc@deloitte.co.uk

Prudential risk

Amarit Bains
Assistant Director
amaritbains@deloitte.co.uk

Faiza Farooq
Director
faizafarooq@deloitte.co.uk

Recovery and resolution, and solvent exit

Henry Basing
Director
hbasing@deloitte.co.uk

Emily Grewcock
Director
egrewcock@deloitte.co.uk

ICARA

Brian Thornhill
Director
bthornhill@deloitte.co.uk

Governance

Henry Hofman
Director
hbhofman@deloitte.co.uk

Tasneem Saiki
Director
tsaiki@deloitte.co.uk

Risk culture

Jessica Sunderland
Director
jessicasutherland@deloitte.co.uk

Integrated assurance

Farsha Amran
Senior Manager
famran@deloitte.co.uk

Cain Brown
Manager
cianbrown@deloitte.co.uk

Remuneration

John Cotton
Partner
jdcotton@deloitte.co.uk

Susannah Hill
Director
suhill@deloitte.co.uk

ESG – Climate risk and disclosures

Hetty van der Wal
Associate Director
hevanderwal@deloitte.co.uk

Sarah Cook
Senior Manager
sacook@deloitte.co.uk

Mortgage rule simplification

Alastair McGeorge
Director
amcgeorge@deloitte.co.uk

Amber Smeaton
Senior Manager
asmeaton@deloitte.co.uk

Motor finance and buy now pay later (BNPL)

Lyndsey Fallon
Partner
lfallon@deloitte.co.uk

Priyesh Kotadia
Assistant Director
pkotadia@deloitte.co.uk

General insurance and premium finance

Farsha Amran
Senior Manager
famran@deloitte.co.uk

Christopher Jamieson
Partner
cjamieson@deloitte.co.uk

Price and value outcomes

Alastair McGeorge
Director
amcgeorge@deloitte.co.uk

John Lonen
Director
jolonen@deloitte.co.uk

Change and transformation

Lee Hales
Director
lhales@deloitte.co.uk

Olga Harte
Senior Manager
oharte@deloitte.co.uk

Operational resilience

Mark Westbrook
Director
markwestbrook@deloitte.co.uk

Vincent Greenaway
Senior Manager
vgreenaway@deloitte.co.uk

Third party risk management

Nicola Hicks
Director
nhicks@deloitte.co.uk

Talal Raja
Senior Manager
traja@deloitte.co.uk

Cyber, data governance and cloud

Yannis Petras
Partner
ypetras@deloitte.co.uk

Poppy Khan
Director
pokhan@deloitte.co.uk

Nanette Gárdos
Associate Director
ngardos@deloitte.co.uk

Rupert Hargrave
Senior Manager
ruphargrave@deloitte.co.uk

Internal audit innovation (GenAI / data analytics)

Owen Jackson
Director
ojackson@deloitte.co.uk

Nanette Gárdos
Associate Director
ngardos@deloitte.co.uk

High performing internal audit functions

Alexandra Rodrigues
Associate Director
arrodrigues@deloitte.co.uk

Philippa Figueiredo
Associate Director
pfigueiredo@deloitte.co.uk

Internal audit standards and QA

Owen Jackson
Director
ojackson@deloitte.co.uk

Daniel Wright
Senior Manager
daniwright@deloitte.co.uk

Global markets

Ed Waller
Director
ewaller@deloitte.co.uk

Margarita Streltses
Senior Manager
mstreltses@deloitte.co.uk

Pensions and investment management

Rob Scott
Director
robscott@deloitte.co.uk

Farsha Amran
Senior Manager
famran@deloitte.co.uk

Additional contributions

Lewy Farrer
Senior Analyst
lewyfarrer@deloitte.co.uk

Luana Sambell
Manager
lsambell@deloitte.co.uk

Kyle Taylor
Assistant Marketing Manager
kstaylor@deloitte.co.uk

Deloitte.