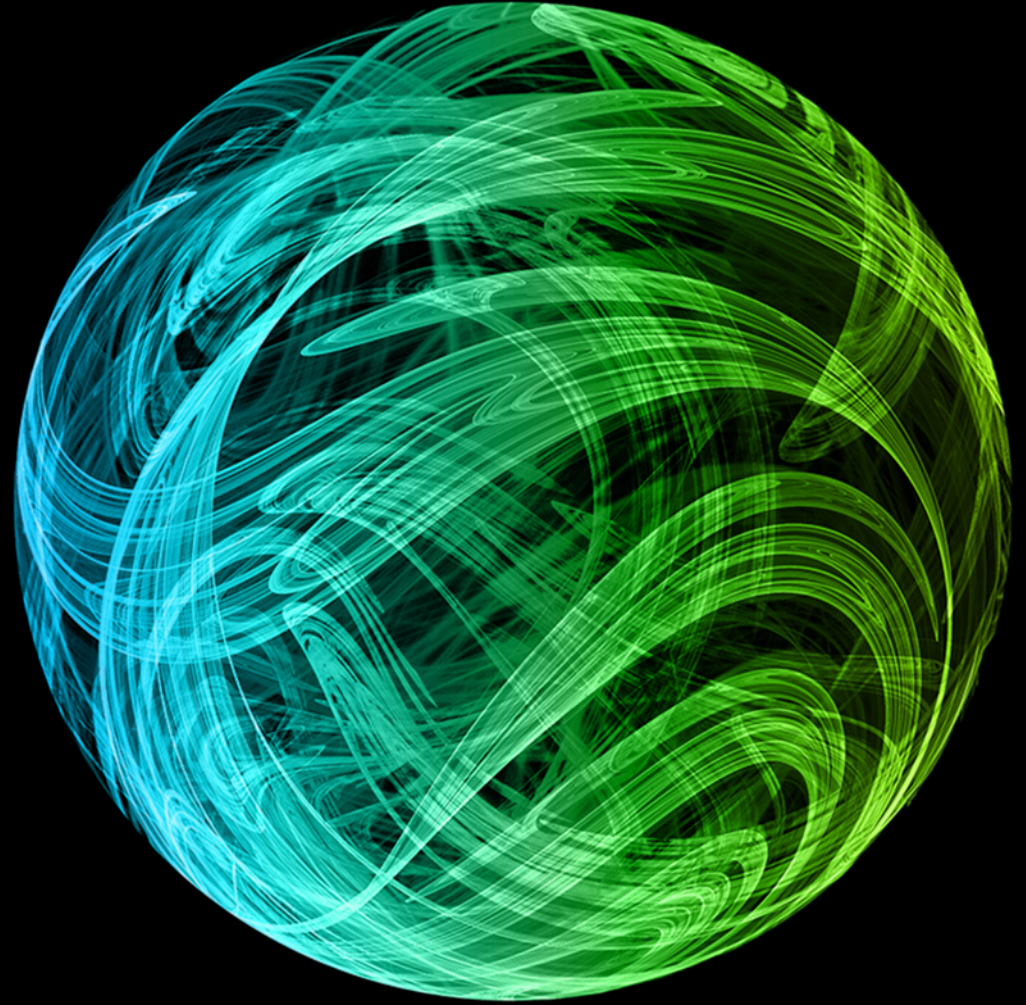




2027 Planning Priorities

Building continuous trust and the evolution of the Three Lines for an AI-enabled future

September 2026

Contents



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

01 Macro considerations and cross-sector

02 Technology and digital

03 Banking and capital markets and investment management

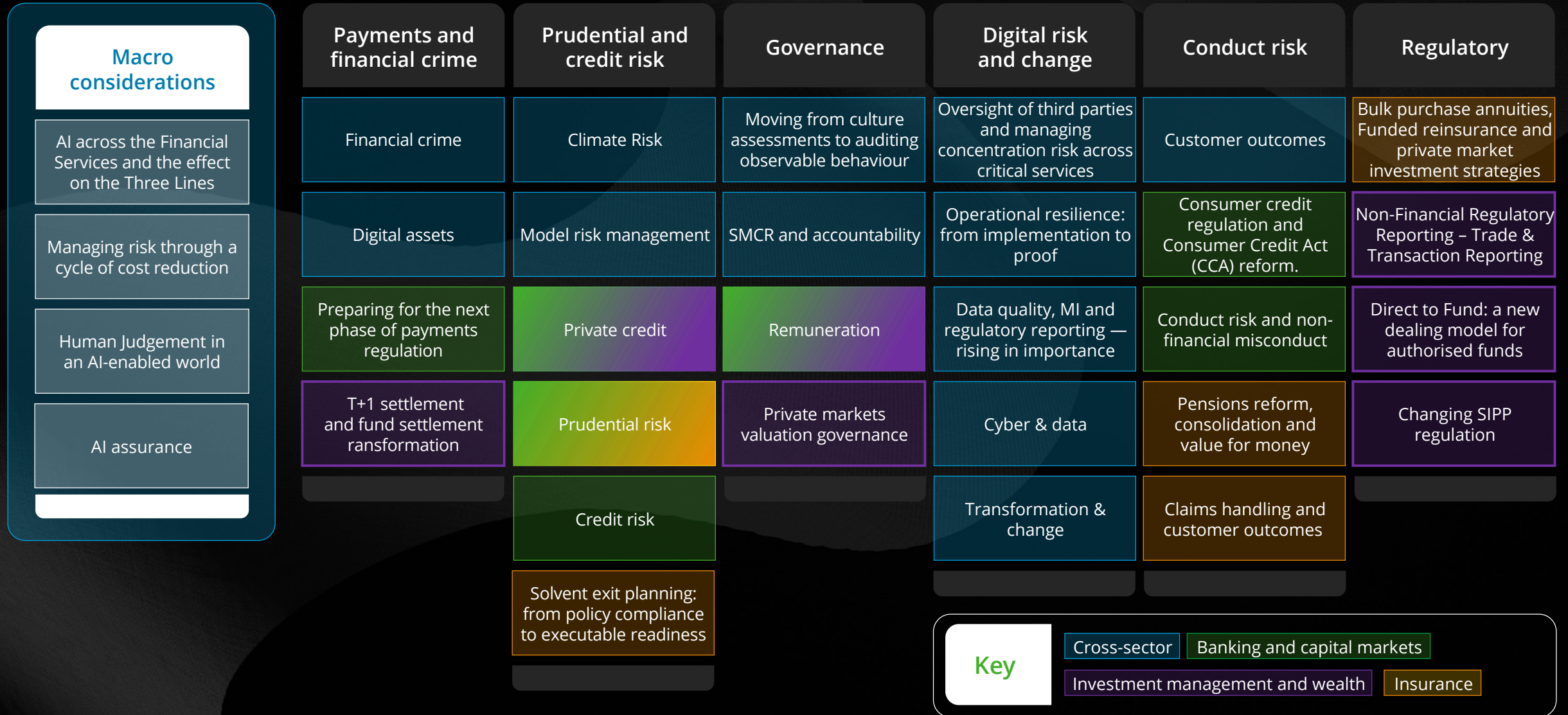
04 Banking and capital markets and insurance

05 Banking and capital markets

06 Insurance

07 Investment management and wealth

Financial services planning priorities topics overview



Macro considerations and cross-sector

01

The financial services landscape continues to be shaped by uncertainty, rapid technological change and evolving expectations from regulators, customers and wider society. For firms, success now depends not only on responding to immediate pressures, but on anticipating how emerging risks will affect strategy, operations, governance and control environments. Two emerging areas are particularly important as firms shape their 2027 internal audit plans: the enterprise-wide adoption of AI across financial services, and the evolution of assurance across the Three Lines of Defence.

Artificial Intelligence is moving from experimentation to enterprise-wide adoption, with wider deployment across customer journeys, operations, decision-making, risk management, financial crime, cyber security, technology delivery and corporate functions. Firms are also exploring increasingly autonomous and agentic capabilities, moving AI from a productivity tool to a core component of how work is performed. As adoption scales, AI is becoming less of a standalone technology topic and more of an enterprise-wide operating model change affecting strategy, people, processes, data, technology and customer outcomes.

This pervasiveness changes the nature of the risk. The challenge is no longer limited to approving individual models or controlling access to generative AI tools. AI may be embedded within vendor products, shared platforms, workflow tools and business processes, while employees and third parties may introduce additional use cases outside established governance routes. The resulting risk profile spans data quality and protection, model performance, explainability, cyber security, operational resilience, third-party dependency, regulatory compliance, conduct and customer outcomes, which we explore across this publication. Firms therefore need a coherent view of where AI is used, what decisions it supports, the outcomes it influences and how those outcomes are monitored.

“AI is moving from experimentation to the heart of how financial services firms operate – reshaping customer journeys, decision-making, risk management and the delivery of services”

How will this impact the Three Lines Model and how risk is managed?

As organisations automate processes and embed AI within workflows, the way risks are managed, controls operate and assurance is produced is changing. Activities that were previously manual and separated across the Three Lines are increasingly connected through digital workflows, automated decision-making, system-generated evidence and more continuous monitoring. Controls and assurance can be designed into the process, with exceptions and performance indicators generated as activity occurs. This may improve the timeliness and reach of assurance, but only where the underlying data, process design, configuration, monitoring logic and accountability can be trusted.

This evolution has distinct implications for each line of defence. The First Line remains accountable for risks, controls and outcomes, including where activity is performed by automated systems or AI agents. However, it will need new capabilities to define acceptable performance, interpret AI telemetry, monitor exceptions and intervene where outcomes fall outside expected parameters. The Second Line will increasingly need to translate risk appetite, policy and regulatory expectations into practical guardrails, standards, monitoring requirements and escalation thresholds that can be embedded within AI-enabled processes. Its role will move closer to the design of the organisation's trust architecture, while retaining effective oversight and challenge.

Internal Audit must continue to provide independent assurance, but its focus and methods will need to evolve. Traditional control testing will remain relevant, particularly where material judgements and manual interventions remain. However, as process execution, control activity and evidence generation become more automated, Internal Audit will need to assess whether the overall system of governance, control, monitoring and assurance is reliable. This includes validating First Line assurance mechanisms, Second Line guardrails and the integrity of the data, technology and human oversight on which they depend. The central question increasingly becomes not only “Did the control operate?”, but “Can we trust the system that generates the decision, evidence and assurance?” Organisations that adapt their assurance models effectively should be better positioned to identify emerging risks earlier, reduce unnecessary duplication across the Three Lines and provide stakeholders with greater confidence that risks are being managed continuously, rather than only at the point of review.

1

Establish whether AI governance provides a reliable foundation for adoption

Effective governance is the essential foundation for safe and responsible AI adoption. The organisation should have a sufficiently complete and current view of how AI is being used across business functions, technology platforms, third parties and by employees, so that management understands its exposure and unmanaged or shadow AI does not develop outside established governance routes. Internal Audit should review whether the organisation can identify and inventory AI use consistently; whether ownership, policies, risk appetite, approval and lifecycle controls are clear and proportionate; and whether board and senior management oversight provides effective challenge as adoption scales. This review should include less visible forms of adoption, such as AI embedded within existing products, employee-led tools and external service providers.

2

Assess whether the Three Lines operating model remains clear and effective

Review whether roles remain clear as AI-enabled activities blur traditional boundaries between process execution, control, monitoring and assurance. The First Line should retain ownership of risks and outcomes and have the capability to monitor automated performance and intervene when required. The Second Line should define effective guardrails, standards and oversight without assuming management ownership. Internal Audit should have sufficient visibility across the organisation and an appropriate seat at the table for significant AI governance, investment and transformation discussions, enabling it to understand the aggregate risk profile, identify gaps or duplication across the Three Lines and form an informed view on whether management is obtaining appropriate assurance. This engagement should support timely independent challenge without Internal Audit assuming responsibility for design or implementation.

3

Rethink how assurance is delivered over AI-enabled processes

Where AI is embedded within business processes, Internal Audit should reconsider how those processes are audited. Assurance should extend beyond traditional control testing to assess whether AI-enabled decisions, automated controls and system-generated evidence can be relied upon. This includes the quality and completeness of the underlying data, the design and performance of the AI, the effectiveness of human oversight, and the monitoring of exceptions, drift and unintended outcomes. Internal Audit may not be able to review every AI-enabled process and should therefore apply a risk-based approach, prioritising those with the greatest potential impact on customers, regulatory obligations, financial reporting, operational resilience or other material outcomes. Audit methods and testing should then be adapted to the nature of the technology and the risks it introduces, rather than applying a standard audit approach to a fundamentally different process.

4

Ensure Internal Audit plans reflect AI as a pervasive risk

Internal Audit should assess whether the audit universe, risk assessment and plan identify AI as a pervasive driver of risk and operating model change, rather than treating it only as a standalone technology review. The plan should provide a coherent view of where AI is embedded across the organisation and prioritise coverage of the use cases and processes with the greatest potential impact on customers, regulatory obligations, financial reporting, operational resilience or other material outcomes. Depending on the risk profile, this may require a combination of dedicated AI reviews, thematic work and AI-related testing within broader business audits. Internal Audit should also keep the plan under review as adoption develops and new material use cases emerge.

5

Build the capability to provide effective AI assurance

Internal Audit should assess whether it has the skills, methodology, data access, tools and specialist support required to provide credible assurance over AI. This will require an appropriate combination of business, risk, data, technology and model expertise, supported where necessary by internal or external specialists. Audit methodology, training and quality arrangements should enable teams to identify AI-related risks, test AI-enabled processes and evaluate whether automated decisions and system-generated evidence can be relied upon. Capability plans should reflect both current needs and the expected pace and scale of AI adoption.



“As AI reshapes risk, the Three Lines must adapt to provide clarity, challenge and confidence”

Marc McNulty

Partner – Internal Audit

Managing risk through a cycle of cost reduction

Given current economic and trading conditions, organisations are under increasing pressure to review their cost base and deliver sustainable reductions without weakening resilience, controls or customer outcomes.

Technology transformation, including AI-enabled automation, outsourcing and offshoring, is increasingly being used to deliver efficiencies; however, these changes may also reduce headcount, shift accountabilities and alter the control environment.

The cumulative impact of cost reduction and technology-led change can weaken governance, control effectiveness, operational resilience or customer outcomes where risk and control frameworks do not evolve at the same pace as the operating model.

As outlined in our From Three Lines of Defence to Continuous Trust topic, organisations are looking to embed more controls, monitoring and assurance activities within day-to-day business processes. This requires Second Line functions to adapt their oversight, governance and challenge as operating models change. Regulators are also expecting firms to demonstrate that these capabilities remain effective, proportionate and resilient despite ongoing organisational change, greater reliance on third parties, and increased use of technology and automation.

1 Regulators increasingly expect risk management to be embedded within transformation programmes by design

Firms should be able to demonstrate that customers are not harmed as a result of transformation, cost reduction or business change. Risk, compliance and customer outcomes must be assessed throughout the design and implementation of efficiency initiatives, including those enabled by AI and automation. This includes evidence that governance fora have provided effective challenge; key risks have been identified and mitigated; and decisions relating to headcount reduction, outsourcing, offshoring, automation and AI adoption have been subject to appropriate oversight and accountability.

3 Control environments can be diluted over time

Cost reduction programmes are often implemented incrementally, making it difficult for firms to identify the cumulative impact on customers, governance and controls. Workforce reductions, organisational restructuring, role consolidation and AI-enabled automation can weaken segregation of duties, reduce subject matter expertise, diminish management oversight or change how controls operate in practice. Regulators increasingly expect firms to understand how the control environment has evolved over time and demonstrate that key risks remain appropriately controlled despite ongoing organisational change.

2 Risk functions must evolve alongside changing operating models

Cost reduction programmes often shift risk rather than remove it. Increased reliance on third parties, automation and AI can create new operational, conduct, technology, data and concentration risks that may not be adequately covered by traditional assurance approaches. Where headcount reductions or role consolidation occur, risk and compliance functions need to demonstrate that monitoring, challenge and oversight activities remain aligned to the firm's evolving risk profile and continue to focus on the areas presenting the greatest risk.

4 Management information must evolve to identify emerging risks and unintended consequences

As operating models become more complex and increasingly reliant on third parties, technology and AI, firms need more sophisticated management information to identify deterioration in service quality, customer outcomes, control effectiveness and operational performance. Regulators increasingly expect firms to monitor the impact of cost reduction and transformation initiatives through outcome-based metrics and risk indicators, enabling management and Boards to challenge whether expected savings have been achieved without creating unintended exposures.

Four things Internal Audit should do

1 Assess whether risk is embedded by design within transformation programmes

Review whether cost reduction, headcount reduction, outsourcing, offshoring, AI and automation initiatives are subject to robust risk assessment, governance and challenge throughout the programme lifecycle. Assess whether risk, compliance, control and customer outcome considerations influence decision-making, rather than being evaluated retrospectively.

2 Challenge culture, behaviours and speaking-up arrangements

Assess whether pressure to deliver efficiencies or reduce headcount has affected escalation practices, independent challenge, risk appetite decision-making, capacity within control functions, or employees' willingness to raise concerns. Firms with strong cultures are more likely to identify and respond to emerging risks before they crystallise.

3 Evaluate whether risk and compliance oversight remains aligned to the evolving risk profile

Assess whether second-line functions have adapted their frameworks, monitoring and assurance activities to reflect emerging risks arising from changing operating models, including headcount reductions, increased third-party dependency, automation and AI adoption. Review how assurance resources are prioritised and whether coverage remains focused on the areas of greatest risk.

4 AI-enabled efficiencies and control impact

Assess whether AI initiatives used to deliver efficiencies are subject to appropriate design authority, data governance, model oversight and post-implementation monitoring. Internal Audit should consider whether automation has changed control ownership, reduced manual review, affected customer outcomes or created new dependencies that require additional assurance.

Human judgement in an AI-enabled world

As artificial intelligence becomes embedded in everyday work, a new challenge is emerging. Not whether organisations can use AI, but whether people continue to think for themselves. AI can generate insights, recommendations, reports and even assurance testing faster than ever before, but it cannot replicate human judgement, ethical reasoning or organisational context. As reliance on AI grows, organisations should consider whether they are developing cultures that encourage curiosity, challenge and accountability, or whether convenience is slowly replacing critical thinking.

1 The real challenge is not whether AI can think, it's whether people stop thinking

AI works best when it strengthens human thinking rather than replacing it. Used well, it can act as a sounding board: helping auditors test assumptions, challenge first impressions, consider alternative explanations and ask better questions. The risk is not the existence of AI, but the possibility that its convenience encourages people to accept outputs too quickly. The internal audit functions that gain most from AI will be those that use it to deepen curiosity, judgement and challenge, while keeping accountability firmly with the auditor.

3 The skills emphasis is shifting from technical execution to human capability

Internal audit functions have invested heavily in technical skills because auditors have needed to understand increasingly complex processes, controls and technologies. As AI takes on more of the heavy lifting of data gathering, summarisation and first-draft analysis, the points of differentiation will shift. Greater value will come from how auditors exercise professional judgement, communicate challenge, interpret context and bring human insight to areas where automated analysis alone is insufficient.

5 Trust is being redefined

For decades, assurance processes have relied on an implicit understanding of what constitutes sufficient evidence and acceptable levels of accuracy. AI is beginning to challenge those assumptions. If a report is largely drafted by AI, what level of review is required? If testing is partially automated, how much validation should be performed? As AI changes how work is produced, organisations must reconsider what it means to trust information, evidence and conclusions. Human oversight is not simply a control requirement. It is increasingly a prerequisite for maintaining confidence in decision-making.

2 Human judgement is about more than accuracy

Judgement is about more than producing accurate outputs. It requires professional scepticism, independence, objectivity, ethical reasoning and a clear understanding of the organisation's risk context. The Global Internal Audit Standards place emphasis on integrity, objectivity, competency and the basis for reliance on internal auditors' work and judgement. AI can support analysis and provide recommendations, but cannot determine whether an audit conclusion reflects the function's values, professional responsibilities or the wider consequences for stakeholders.

4 Critical thinking is developed through interaction, not training alone

Human skills will not develop through formal training alone. Auditors build judgement by seeing how others approach uncertainty, frame problems, challenge evidence and adapt their thinking as new information emerges. Coaching, peer review, debate and exposure to different perspectives help create the confidence to ask difficult questions. As AI changes how audit work is performed, functions will need to be deliberate about creating everyday interactions that strengthen curiosity, professional scepticism and practical judgement.

Five things Internal Audit should do

1 Assess whether ethical considerations remain central to decision-making

Review whether AI-enabled activities continue to support organisational values, ethical expectations and accountability frameworks. The focus should extend beyond compliance and accuracy to consider fairness, transparency and responsible decision-making.

2 Evaluate whether challenge is embedded within AI-enabled processes

Assess whether individuals understand their responsibility to review, question and challenge AI-generated outputs. Human-in-the-loop controls should be designed to promote meaningful judgement rather than passive approval.

3 Revisit assumptions around evidence, accuracy and reliance

Evaluate whether existing audit methodologies, testing approaches and quality assurance practices remain appropriate as AI increasingly supports the creation of work products and assurance evidence.

4 Foster curiosity and learning across the function

Create opportunities for auditors to learn from different disciplines, perspectives and experiences. Encourage behaviours that reward inquiry, constructive challenge and exploration rather than simply reaching answers quickly.

5 Strengthen critical thinking as a core professional capability

Critical thinking should not be viewed as a standalone training topic or a skill reserved for senior auditors. It should be embedded throughout recruitment, coaching, methodology and performance development. In a world where answers are increasingly abundant, this is where Internal Audit gives value: by asking the questions that others overlook, challenging what appears certain and applying judgement to the areas where AI alone cannot provide assurance.

AI assurance

AI is no longer a discrete system to be reviewed in isolation; it is becoming a feature of the wider technology backbone of organisations and their control environment. It is increasingly embedded in enterprise platforms, vendor products, customer journeys, credit decisions, and the tools functions use themselves. Where organisations have not formally enabled AI, employees have often found ways to use it outside of approved channels. For audit, this changes the assurance approach. A single annual AI review can provide only partial comfort over a technology that may now permeate the full risk universe. For 2027, the more useful ambition may be to make AI a standing consideration in every auditable entity and audit.

1 Not (only) a technology risk

For Audit Executives, the message is clear: the risk is pervasive (not purely a ‘technology’ one), many functions are still defining their AI assurance approach, and a single AI audit will not be enough. Key risks for FS organisations, including governance and strategy, data quality and provenance, and agentic AI, cut across multiple parts of the audit universe. A function that reports “we have audited AI” may therefore be providing narrower assurance than the Audit Committee expects.

3 The advent of ‘shadow AI’

The continued prominence of AI reflects four linked pressures: *regulatory attention; rapid business adoption / scaling; evolving compute and technology capability; and increased employee use*. Organisations are already using AI to improve productivity, service quality and decision-making, often before governance, monitoring and accountability have fully matured. In parallel, employees use public or embedded AI tools outside approved (authorised and safe) channels, creating risks around data protection, intellectual property, output quality and transparency.

5 AI and Internal Control over Financial Reporting: the focus of external auditors

External auditors have also started to actively scrutinise AI governance, with the recently published COSO guidance setting clear expectations for controls and evidence. Unlike deterministic tools, GenAI is probabilistic – outputs can vary and be difficult to explain, introducing reliability and validation challenges. Relevant controls over risks relevant to 2026 year-end Financial Reporting need to be identified and scoped in accordingly.

2 The regulatory environment

Regulatory scrutiny of AI continues to accelerate across both the UK and US. The implementation of the EU AI Act is increasing expectations around governance, accountability, transparency and risk management for AI-enabled solutions, while global regulators are increasingly signaling that existing frameworks relating to operational resilience, conduct, model risk management and customer outcomes should be applied to AI use cases. PRA suggests that use cases will be assessed through existing prudential, model risk management, conduct, operational resilience, and existing data protection frameworks. Internal audit must ensure AI systems comply with this broader regulatory landscape, and the IA plans need to reflect this reality.

4 AI and data

High-quality data is fundamental for effective AI, underpinning transparency, model validation, explainability, fairness, and cybersecurity. Internal audit needs to assess data provenance, relevance, representativeness, and bias mitigation, especially given the EU AI Act’s expectations for high-risk systems. The focus should be on robust frameworks are in place for deployment, including clear risk appetite, strong internal controls, and accountability for outcomes.

Five things Internal Audit should do

1

Embed AI into audit planning and scoping

Treat AI as a standing consideration across the audit universe, not only as a standalone review. Each engagement should ask whether AI is used, whether it affects existing controls, what decision it influences, who approved it, what data it consumes, and whether outputs can be explained.

2

Apply existing risk principles while standards catch up

AI regulation and standards, particularly for emerging agentic capabilities, are still developing, so internal audit should not wait for perfect guidance. AI use cases need to be assessed through existing prudential, model risk management, conduct, operational resilience, and data protection frameworks (e.g., GDPR). Existing principles around risk appetite, accountability, change control, data governance, model risk, third-party risk and customer outcomes should be applied consistently to AI use.

3

Provide a clear AI assurance view to the Audit Committee

Internal audit should help the Audit Committee understand where AI is being used, where assurance has been provided, and where material gaps remain. IA teams should look to advise the business on finding the balance between risk management, governance, and efficiency – helping the business safely streamline their transformation capabilities so governance manages risk but is not a bottleneck. For both advisory and assurance reviews, IA teams should consider new AI risks, existing IT processes and digital monitoring opportunities

4

Challenge how management responds to AI demand signals

Shadow AI can indicate un-met business need, but it also exposes gaps in governance, training and approved tooling. Internal audit should assess whether management has identified these demand signals and put in place proportionate routes for safe adoption, including sufficient guardrails, while challenging risks around ungoverned IT.

5

Strengthen AI capability within internal audit

Audit Committees are not only asking for assurance over the enterprise but are asking IA departments to become more efficient using and enabling themselves with the capabilities. The mature IA function will be able to assure and advise the business on AI implementations and risk management. Teams need sufficient fluency to challenge how models are selected, prompted, monitored and retired. Using AI within the audit process, under appropriate governance, can help auditors understand the risks and provide more practical findings.

Customer outcomes

Since the introduction of Consumer Duty, the FCA has continued to reinforce its expectation that firms should demonstrate that customers are receiving good outcomes. During 2027, regulatory focus is expected to remain on the use of data, management information and outcome testing to provide Boards with clear evidence that products and services consistently deliver good customer outcomes across the customer lifecycle, and that firms can identify and mitigate potential harm.

1 Customer Outcomes, and how these are monitored, remain a key priority of the FCA

Firms are expected to move beyond process and compliance-based measures and demonstrate that in practice good outcomes for customers are achieved. This has been evidenced by multiple publications by the regulator across sectors, most recently in July 2026.

3 Increasing focus is placed on Board accountability

Boards and senior management must be able to evidence effective oversight and challenge, supported by reliable information that enables them to assess whether appropriate customer outcomes are being achieved across products and services.

5 Regulators are increasingly testing firms' evidence

Firms must be able to demonstrate how insight from data and monitoring activities drives decision making, remediation and continuous improvement, rather than relying solely on policy and framework documentation.

Internal Audit functions should provide independent assurance over the effectiveness of customer outcome frameworks and the quality of information supporting Board oversight. Particular attention should be given to whether firms can evidence a clear link between customer outcome monitoring, management action and resulting improvements in customer experience. Audit plans should include focus on outcome-based testing and the effectiveness of governance arrangements supporting Consumer Duty compliance, including specific activities to assess the creation, review and challenge of the annual Consumer Duty Board report and other ongoing monitoring activity.

2 Data-driven decision making is increasingly important

Firms are expected to use meaningful management information, customer outcome metrics and trend analysis to identify potential harm, monitor performance and support timely intervention where required.

4 Outcome monitoring should cover the entire customer journey and consider outcomes across customer groups

Firms are expected to consider outcomes from product design through to servicing, complaints handling, forbearance and customer support, and ensure that outcomes are monitored across customer groups with a particular focus on vulnerable customers and others at greater risk of harm.

“During 2027, regulatory focus is expected to remain on the use of data, management information and outcome testing”

Five things Internal Audit should do

1 Outcome monitoring framework

Assess whether the customer outcome monitoring framework is comprehensive, clearly defined and aligned to Consumer Duty expectations. This should have coverage across the customer journey and customer segments.

2 Management information and metrics

Review the appropriateness of customer outcome metrics, key risk indicators, thresholds and escalation processes used to identify actual or emerging customer harm.

3 Data quality and governance

Evaluate the accuracy, completeness and timeliness of data used to support customer outcome reporting and Board decision making. Internal audit technology and data analytics should be used to deliver this insight more quickly and comprehensively and enable greater insight into the quality of data.

4 Board oversight and challenge

Assess whether governance forums receive sufficient information to effectively oversee customer outcomes and demonstrate appropriate challenge and decision making.

5 Remediation and continuous improvement

Review how customer outcome issues are identified, escalated, tracked and remediated, including whether lessons learned are used to improve products, services and customer journeys.

Oversight of third parties and managing concentration risk across critical services

Building on the Customer Outcomes topic, firms remain accountable for customer outcomes regardless of whether activities are performed internally or by third parties. As a result, regulators are increasing their focus on third-party dependency, concentration and operational resilience risks, with expectations that firms maintain effective oversight of critical suppliers and retain clear accountability for customer outcomes and compliance.

The designation of UK Critical Third Parties (CTPs), the mandatory IIA Third-Party Topical Requirement, and forthcoming Material Third-Party Reporting requirements are collectively raising expectations for governance, dependency mapping, resilience and concentration-risk oversight. Firms will also face enhanced regulatory reporting obligations for material third-party arrangements and the governance supporting them

1 Understanding end-to-end dependency chains

Regulators increasingly expect firms to understand the full dependency chain supporting important business services, including fourth parties, offshore operations, intra-group arrangements, cloud providers and AI-enabled services. This requires comprehensive dependency mapping to identify critical dependencies, assess impacts and establish contingency arrangements.

3 AI is creating a new class of third-party and concentration risks

As AI adoption accelerates, regulators are focusing on associated governance, resilience, data and concentration risks. Firms may become dependent on a small number of AI providers, foundation models or embedded AI solutions. They should understand where AI supports important business services, how suppliers use AI and whether frameworks address model failure, explainability, data usage, bias, cyber threats and compliance.

5 Accountability must be supported by effective ongoing oversight

Firms remain accountable for customer outcomes and regulatory compliance regardless of outsourcing arrangements. The FCA expects effective oversight through governance, meaningful management information, performance monitoring and timely intervention, particularly for critical or customer-facing services. There is increasing focus on continuous monitoring rather than periodic supplier reviews, in some cases supported by AI-enabled tools.

2 Concentration risk has become a key supervisory concern

The designation of the first UK Critical Third Parties (CTPs) in July 2026 reinforces a systemic focus on the resilience of supply chains and extended enterprise ecosystems. Regulators are placing greater emphasis on reliance on a small number of cloud, technology and service providers. Firms are expected to identify common dependencies and single points of failure, assess provider resilience and substitutability, and understand concentration risk through fourth parties and wider supply chains.

4 Data quality, exit planning and resilience testing are central

Effective oversight relies on complete and accurate third-party data, including performance, conduct, cyber and resilience metrics. Regulators increasingly expect critical third parties to be included in scenario testing, contingency and exit planning, with governance information supporting timely intervention where service quality or resilience deteriorates.

Five things Internal Audit should do

1 Third-party governance, oversight and accountability

Assess whether governance, monitoring and escalation arrangements provide effective oversight of third-party risks and support requirements around Consumer Duty, SYSC8 (Material Outsourcing) and broader regulatory expectations.

2 Dependency mapping, concentration risk and critical technology dependencies

Assess whether end-to-end dependencies across critical services are mapped, including fourth parties, cloud, AI-enabled services, offshore operations and intra-group arrangements. Review how concentration risks, single points of failure, cyber risks and critical technology dependencies are identified, monitored and escalated, including dependencies on Critical Third Parties.

3 Resilience, contingency and exit planning

Review whether critical third parties are incorporated into scenario testing, incident management, contingency planning and exit strategies, and whether these arrangements have been tested.

4 Material Third-Party Reporting readiness

Assess preparedness for the new reporting regime, including governance, inventories, materiality assessments, dependency mapping and incident reporting processes.

5 IIA Third-Party Topical Requirement conformance

Review whether Internal Audit methodologies, planning and assurance activities have been updated to address third-party governance, risk management and controls across the full supplier lifecycle.

7 Moving from culture assessments to auditing observable behaviour

Overview

Five things you should know about the topic

While culture has for many years been considered an important factor in Internal Audit, it has often been difficult to measure and assess reliably. The new IIA Organisational Behaviour Topical Requirement aims to address this challenge by reframing culture, towards observable behaviours that can be evidenced, tested and audited. The focus is on what people actually do, rather than what an organisation says it is. Importantly, the Topical Requirement introduces a mandatory minimum baseline for assessing organisational behaviour through governance, risk management and controls.

1 Organisational behaviour is not the same as culture

It focuses on the observable choices employees make in their day-to-day roles and interactions with others. As a subset of culture, it gives Internal Audit a practical basis for testing how behaviours are shaped by systems such as performance reviews, recruitment, incentives, training and escalation processes.

3 Behavioural insights require broader evidence

Assessing organisational behaviour requires more than reviewing policies and procedures. Internal auditors should consider a combination of qualitative and quantitative information, such as employee surveys, whistleblowing reports, complaints or focus groups and retrospectives or lessons learned outputs, to build a more complete picture of behaviours present and under the requirement, will require a clear understanding and identification of “organisational objectives” (as per item 1 below).

5 Organisational behaviour can be embedded into existing audits

Behavioural considerations can be incorporated into a variety of reviews, allowing auditors to assess whether organisational behaviour is supporting or hindering the achievement of objectives across a wide range of audits.

2 Behavioural risk is now a defined audit consideration that can be tested using traditional audit techniques

The requirement becomes effective on 15 December 2026, meaning Internal Audit functions should consider it during FY2027 planning and audit activity. The Topical Requirement establishes a minimum baseline for assessing governance, risk management and controls related to organisational behaviour, defining behavioural risk as behaviour that is inconsistent with organisational objectives. Poor behaviours can weaken controls and expose organisations to risk, even where formal frameworks appear robust.

4 Behaviour often explains why controls fail

Many governance and control failures originate from human behaviour rather than control design. Factors such as poor accountability and low psychological safety can create risks that are difficult to identify through traditional control testing.

“Importantly, the Topical Requirement introduces a mandatory minimum baseline for assessing organisational behaviour through governance, risk management and controls”

Five things Internal Audit should do

1 Define expected behaviours

Assess whether the organisation has clearly defined the behaviours required to support its objectives, values and risk appetite. Internal Audit should check for embedded expectations within a large range of evidence.

2 Broaden scope of evidence

Move beyond policies and procedures by using a wider range of behavioural evidence, including observation, interviews, focus groups, employee survey data, complaints, whistleblowing themes and behavioural indicators – such as speak-up trends, attrition data, conduct events and absence data – and retrospectives or lessons learned outputs. Auditors should have appropriate facilitation skills so that discussions are well managed and generate reliable insight into how people behave in practice. IA should consider how data and technology (including AI) can be factored in for cultural assessment and measurement.

3 Identify behavioural root causes and evaluate behavioural drivers

Assess whether behavioural factors contribute to governance, risk or control weaknesses to understand the causes of issues, not just the symptoms. Report findings using evidence-based observations focused on behaviours, impacts and improvement opportunities. Evaluate whether organisational mechanisms, including incentives, performance measures, leadership actions, recognition and consequences, reinforce the behaviours needed to achieve desired outcomes.

4 Embed behavioural insight into the audit plan

Internal Audit should define how organisational behaviour and culture assurance will be owned and delivered across the audit plan, whether through dedicated reviews, embedded coverage, or a hybrid model. A consistent framework of behavioural indicators and data-led insights, such as conduct events, speak-up themes, training completion and mandatory leave, should be applied across relevant audits. This enables Internal Audit to assess whether behaviours support or undermine controls, decision-making and customer outcomes.

5 Reporting on Organisational Behaviour

Internal Audit’s work on risk culture and organisational behaviour should inform the annual conclusion, highlighting common risks and impact on firm objectives. A key challenge is defining ownership; while culture is broad, audit action plans need practical timeline and clear management accountability. Fixing these issues should not be a one-time event. IA teams should debrief in a team setting on the identified issues and apply behavioural insights across IA’s work linking findings by common themes.

SMCR and accountability

Accountability remains a cornerstone of the regulatory regime and a critical component of effective governance, risk management and organisational culture. During 2026, the FCA, PRA and HM Treasury implemented the first phase of reforms to the Senior Managers and Certification Regime (SM&CR), introducing measures intended to simplify the regime, reduce administrative burden and improve proportionality. These included streamlining a number of processes and providing additional guidance on the application of the regime. Further consultation on more fundamental legislative reforms, including the scope of the certification regime and the approach to SMF approvals, is expected later in 2026.

1 Simplification without dilution

The 2026 SM&CR reforms are intended to reduce administrative complexity, not weaken accountability. Firms must still evidence clear responsibilities, effective governance and active management of key risks, with regulators continuing to view accountability failures as a driver of conduct, risk and governance breakdowns.

3 Change reshapes accountability

Organisational change, including operating model transformation, outsourcing, AI adoption and regulatory simplification, can alter decision rights, reporting lines, control ownership and risk oversight. Accountability frameworks should be updated alongside change to avoid gaps, overlaps or ambiguity.

5 From compliance to outcomes

Against this backdrop, and as firms implement the SM&CR reforms, they should consider whether their wider accountability frameworks remain effective, embedded and capable of supporting sound governance. The emphasis should extend beyond technical compliance to how accountability shapes behaviours, decisions, risk management and outcomes.

2 Accountability beyond the framework

Regulatory expectations are also moving beyond formal structures to focus on behaviours, culture and decision-making. Accountability must therefore be demonstrable in practice, not just through documentation.

4 AI raises new ownership challenges

AI creates specific accountability challenges where automated tools support decisions, risk assessment, customer interactions or control activities. Firms need clear ownership of AI risks, defined governance and human oversight, and accountability across business, technology, data, risk and compliance teams.

“Regulatory expectations are also moving beyond formal structures to focus on behaviours, culture and decision-making. Accountability must therefore be demonstrable in practice, not just through documentation”

Five things Internal Audit should do

1 Incorporate SM&CR reform implementation into planned reviews

Where SM&CR reviews are already planned, incorporate coverage of management's implementation of recent reforms and determine whether revised processes, governance arrangements and controls remain compliant with regulatory requirements. Given the scale of the changes, this may not warrant a standalone review in all firms, but internal audit should assess whether there is sufficient visibility over the impact of future reforms.

2 Assess clarity of accountability frameworks

Assess whether responsibilities remain clear, current and aligned to the firm's operating model and regulatory obligations. Challenge overlaps, gaps or unclear ownership of material risks, and use wider audit reviews to consider whether accountabilities support effective governance, oversight and control.

3 Test accountability in practice, conduct and culture

Through interviews, committee observations and decision reviews, evaluate whether senior individuals demonstrate effective ownership, challenge, escalation and oversight of key risks and regulatory issues. Assess whether accountability expectations are embedded within performance management, remuneration, conduct frameworks and risk culture initiatives, and whether management uses culture data to identify and respond to accountability failings.

4 Review governance over organisational change

Assess whether major transformation programmes, outsourcing arrangements and organisational restructures include appropriate accountability design and governance oversight. This may include how accountability for material change is assessed and allocated, whether the right skills, knowledge and capacity are in place, and whether governance across the transformation portfolio reflects programme materiality and Board oversight requirements.

5 Assess AI accountability and oversight

Review whether AI use is subject to clear ownership, governance and human oversight, particularly where it supports decisions, customer interactions, risk assessments or control activities. Assess whether accountability for AI-related risks is understood across business, technology, data, risk and compliance teams, and whether escalation routes and senior management oversight are effective.

Financial crime

Financial crime, encompassing areas such as money laundering, terrorist financing and corruption, remains a cross-sector priority. Its scale and sophistication are growing due to the use of AI, evolving typologies and a rapidly changing geopolitical environment. Organisations across all sectors face increasing regulatory scrutiny and penalties for failing to prevent financial crime. Internal audit plays a critical role in providing independent assurance that frameworks are robust, proportionate, and effective. This ensures organisational integrity, safeguards stakeholder trust, and maintains a strong defence against increasingly sophisticated criminal activity.

1 Industrialisation of threat

Generative AI, deepfakes, and synthetic identities are lowering the cost and raising the credibility of fraud and social engineering attacks. Real-time payments compress the window for detecting suspicious activity, while digital assets and complex global supply chains create new avenues for money laundering and sanctions evasion. Organisations should explore opportunities to use AI-powered tools to tackle increasingly sophisticated, AI-enabled financial crime.

3 Heightened corporate accountability

Regulatory frameworks across major jurisdictions increasingly hold organisations responsible for failing to prevent financial crime, not just for committing it. This includes new "failure to prevent" offences (e.g., fraud) and the provisions within the new EU anti-corruption legislation, which introduces or strengthens corporate liability for corruption. Large organisations now face direct corporate liability for failing to maintain reasonable prevention procedures. This trend demands demonstrable proactive prevention measures and places significant onus on corporate governance and senior management.

5 Multi-dimensional cost of failure

Beyond direct financial losses, organisations face significant regulatory penalties, costly remediation efforts, criminal liability for the entity and senior individuals, and lasting reputational damage, underscoring the imperative for effective prevention.

2 Evolving regulatory landscape

The regulatory environment is significantly transforming, with UK's "failure to prevent" offences, the EU's new AML package (including a new AMLA and single rulebook) and the recently adopted EU anti-corruption legislation (aiming to harmonise and strengthen the fight against corruption) all expanding in scope and tightening requirements. Key developments include MLR 2026 adjustments to customer due diligence (CDD) / enhanced due diligence (EDD) triggers, the transition of professional services AML/CTF supervision to the Financial Conduct Authority (FCA), and the integration of crypto-service expectations within the Financial Services and Markets Act (FSMA). Corporate transparency is also being enhanced via phased identity verification at Companies House and updated guidance for digital identity (eID) tools. This necessitates a proactive and adaptive approach to compliance for any organisation operating across borders.

4 Third-party exposure

Financial crime risks frequently flow through third-party networks, including agents, intermediaries, contractors, and outsourced providers. Organisations are liable for the conduct of these "associated persons," making robust due diligence and continuous monitoring of the extended enterprise critical.

Five things Internal Audit should do

1

Assess evolving risk landscape

Critically evaluate the organisation's financial crime risk assessment framework, ensuring it adequately identifies and responds to new typologies (e.g., AI-driven fraud, digital assets) and evolving geopolitical risks.

Review the effectiveness of horizon scanning processes for emerging financial crime threats and regulatory changes.

2

Assure "Failure to Prevent" frameworks

Independently assess the design and operational effectiveness of the organisation's "failure to prevent" procedures, particularly for fraud, bribery, and tax evasion, ensuring they align with regulatory expectations and industry best practices.

Verify that the six guiding principles (top-level commitment, risk assessment, proportionate procedures, due diligence, communication/training, monitoring/review) are embedded and effective. (Source: Chapter 3 of Economic Crime and Corporate Transparency Act 2023 – updated 10 October 2025)

3

Evaluate third-party risk management

Review the robustness of due diligence, contractual protections, and ongoing monitoring processes for third parties and associated persons, ensuring the financial crime framework extends effectively across the extended enterprise.

Assess controls designed to mitigate sanctions and corruption risks flowing through third-party networks.

4

Review data, technology & analytics governance

Assess the governance, explainability, and data quality of AI-driven monitoring tools and other defensive technologies used to combat financial crime.

Verify that alerts are cleared effectively and that the organisation is leveraging and governing AI responsibly.

5

Challenge organisational culture & response

Evaluate the effectiveness of the organisation's financial crime culture, including tone from the top, speak-up mechanisms, and training programmes for high-risk roles.

Review investigation capabilities and regulatory reporting processes (e.g., SARs), ensuring lessons from incidents and near-misses are effectively integrated into the framework.

Digital assets and blockchain technologies are transforming both the investment and payments landscape, with growing activity across tokenised securities, stablecoins and tokenised deposits. Regulatory developments are providing firms with greater confidence to move from pilots and proofs of concept towards live deployment and scale. As activities scale, it is important that 2LOD and 3LOD provide effective review and challenge. This means understanding not only the technology but also evolving regulatory expectations, risk profiles and product characteristics. Building specialist digital assets capability in internal audit is therefore becoming critical in order to keep pace with business developments.

1 Adoption is accelerating as regulatory clarity improves globally, although strategies vary greatly

Firms are exploring a range of use cases, including the issuance, distribution and custody of tokenised securities and funds; digital cash solutions for payments, settlement and collateral management, including tokenised deposits and stablecoins; and crypto custody and trading services. As activity grows, firms face the challenge of scaling governance, risk management, control frameworks and specialist capabilities in line with business expansion. Risk exposures vary significantly depending on the business model, products offered and use cases, requiring a tailored and proportionate approach to oversight.

3 UK policymakers' attention is shifting to stablecoins and tokenised deposits in payments

Further reforms to bring UK-issued stablecoins (and tokenised deposits) within payments regulation should support the further development of a UK stablecoin payments market, by attaching clearer rights and protections for users and businesses. However, implementation of these payments reforms is unlikely before 2029, with significant policy development expected through 2027-28.

5 The regulatory landscape continues to evolve internationally

US developments remain a key focus, while the EU's review of the Markets in Cryptoassets Regulation (MiCA) signals that the EU framework will continue to evolve despite now being in application. Proposed MiCA changes could emerge in H2 2027, requiring firms to further adapt compliance frameworks, controls and operating models over time.

2 UK FCA crypto and stablecoin licensing programmes are a near-term priority for regulated firms and crypto natives alike

Many regulated firms will likely need a variation of permission (VoP) to launch crypto and stablecoin offerings. With the VoP and authorisation application window open for just five months from end-September 2026, is crucial for firms to demonstrate effective governance, robust controls and plans to ensure compliance by October 2027.

4 Scaling tokenised capital markets from experimentation to live activity is another focus

The Bank of England and FCA set out their vision for UK wholesale markets in May 2026, with a final roadmap expected by year-end and consultations on potential rule changes expected in 2027. However, there is growing recognition that industry, Government and regulators need to work together to scale live activity. The UK industry tokenised repo trial, targeted for Spring 2027, aims to move activity beyond pilots and create the momentum needed to support investment in tokenised markets.

“As activity grows, firms face the challenge of scaling governance, risk management, control frameworks and specialist capabilities in line with business expansion”

Five things Internal Audit should do

- 1 Understand the organisation's digital assets strategy and risk profile**
 Develop a clear understanding of the organisation's digital assets strategy, use cases, industry pilot activity, interoperability functionality being developed (provision of wallets for example) and level of exposure. Assess how risks such as financial crime, market, conduct, technology, cyber, third-party, legal, capital and liquidity risks manifest across different products and business models and reflect these in audit planning.
- 2 Embed digital assets into risk assessment and audit planning, supported by continuous monitoring**
 Integrate digital assets into Internal Audit risk assessments and annual plans, supported by continuous monitoring of emerging products, business activities and risk exposures. As adoption accelerates, Internal Audit should adapt assurance coverage dynamically and provide independent challenge at critical stages of the lifecycle, including design, implementation and pre-launch activities, while maintaining appropriate independence.
- 3 Assess regulatory readiness across jurisdictions**
 Evaluate whether governance, controls and compliance frameworks are keeping pace with evolving regulatory expectations. Internal Audit should assess how regulation applies to the firm's activities across relevant jurisdictions, including cross-border use cases. While jurisdiction-specific considerations remain important, firms may be able to leverage common risk and control themes when designing assurance coverage.
- 4 Build and access specialist capabilities**
 Assess whether Internal Audit has the knowledge and skills required to provide effective assurance over digital assets activities. This may require targeted training, certifications, or external specialist subject matter expertise as firms expand activity and risk exposure in this rapidly evolving area.
- 5 Assess the full spectrum of risks associated with the firm's digital assets activities**
 Internal Audit should tailor coverage to the specific products, services and use cases being pursued, considering not only technology risks but also others such as regulatory, strategic, financial crime, conduct, custody, operational resilience, third-party, legal and governance risks. The relative importance of these risks will vary across business models and activities.

Climate and environmental risks continue to exist on board and regulatory agendas as firms face increasing scrutiny over their ability to identify, assess and manage the financial and operational impacts of climate change. Regulators are placing greater emphasis on how climate-related risks are integrated into governance, risk management, strategic planning and capital frameworks, rather than treating them as standalone sustainability programmes, as set out by the Prudential Regulation Authority's (PRA) Supervisory Statement 5/25 'Enhancing banks' and insurers' approaches to managing climate related risks' and the European Central Bank's 'Good practices for climate and nature risk management'. Internal Audit functions should assess whether climate and environmental risks are embedded within existing risk management processes, supported by robust challenge, appropriate data and credible scenario analysis.

1 Regulators increasingly expect climate risk to be treated as a driver of existing risk categories

Both the PRA and ECB emphasise that climate-related risks should not be managed as a separate risk type. Instead, firms should understand how physical risks and transition risks impact existing risk categories such as credit risk, market risk, operational resilience, liquidity risk and reputational risk. The PRA expect firms to apply judgement to embed litigation risks within the firm's risk management.

3 Scenario analysis is becoming a core management tool rather than a regulatory exercise

Both UK financial services regulators place significant emphasis on climate scenario analysis as a key tool for understanding business model resilience and supporting strategic decision-making. Firms are increasingly expected to demonstrate how scenario analysis informs business strategy, risk appetite, capital adequacy assessments and management actions.

Importantly, regulators acknowledge uncertainty and encourage firms to combine quantitative techniques, narrative-based scenarios and expert judgement where appropriate. The focus is shifting from producing scenarios to demonstrating how scenario outputs influence business decisions.

5 Boards are expected to play a more active role in climate risk management

Regulators increasingly expect boards to understand climate-related risks, challenge management assumptions and oversee how climate risks are reflected in business strategy, risk appetite and decision-making. Climate risk is no longer viewed as a specialist topic delegated solely to sustainability functions.

2 Materiality assessments are becoming more sophisticated and forward-looking

Climate and environmental risk assessments are increasingly moving beyond high-level sector assessments towards more granular analysis of geographies, sectors, counterparties, supply chains and collateral exposures. Leading institutions are supplementing traditional risk assessments with scenario analysis, portfolio alignment assessments, physical risk mapping and concentration analysis to identify exposures that may not be visible through traditional approaches. A key expectation emerging from both publications is that firms should be able to explain and evidence how climate risks were assessed, why risks were deemed material or non-material, and how those conclusions influence risk management activities.

4 Climate risk is increasingly linked to operational resilience and third-party risk

A notable theme within the PRA and ECB publications is the increasing recognition of climate-related risks to operational resilience. Physical climate events can disrupt facilities, personnel, data centres, critical services and third-party providers. Firms are increasingly expected to consider whether severe weather events and longer-term climate trends could compromise their ability to deliver important business services.

This extends climate risk beyond financial exposures and into existing operational resilience, outsourcing and third-party risk frameworks.

Five things Internal Audit should do

1 Assess whether climate risks are fully integrated into enterprise risk management

Review whether climate-related risks are embedded within existing risk taxonomies, risk assessments, risk registers and risk reporting rather than being managed separately through ESG programmes.

2 Evaluate governance, accountability and board oversight

Assess whether responsibilities for climate risk management are clearly defined, management information supports effective challenge and boards are appropriately overseeing climate-related risks and strategic responses.

3 Review materiality assessment methodologies

Evaluate whether the organisation has a robust and repeatable process for identifying, assessing and periodically reassessing material climate and environmental risks, including emerging concentrations and interconnected risks.

4 Assess the effectiveness of climate scenario analysis

Review whether scenario analysis is appropriately designed, supported by suitable assumptions and data, and used to inform decision-making across strategy, risk appetite, capital and business planning processes.

5 Evaluate operational resilience and third-party risk implications

Assess whether climate-related risks have been incorporated into operational resilience assessments, business continuity planning, outsourcing oversight and third-party risk management frameworks.

Technology and digital

02

12 Model risk management

Overview

Model risk management (MRM) has been an area of supervisory focus for many years; many firms across financial services have been strengthening their control environments in parallel with making greater use of models. The discipline is undergoing a significant transformation due to the increasing power of generative and agentic AI; these technologies have the potential to increase process efficiency, (e.g. on model validations), while at the same time increasing the governance needs on firms as the AIs themselves generate model risks that must be managed.

As such, the interaction of MRM and AI governance is an area of focus for many firms who seek pragmatic governance models. Advanced firms are also aligning their End user Developed Application (EUDA) frameworks, as many of the risks and controls applicable to EUDAs are similar to those for models.

Five things you should know about the topic

1 SS1/23 compliance

In banking, the PRA continues their detailed reviews of firm's MRM frameworks in order to assess compliance vs. their Supervisory Statement 1/23, Model Risk Management Principles for Banks. The large banks who are in-scope of this supervisory statement will likely be subject to further scrutiny in 2027 regarding the design and implementation of their frameworks.

3 Use of automation

Tooling and automation, both GenAI-assisted and traditional, is an area of heavy focus for many firms, who are looking to speed up model management activity in both the 1st and 2nd lines of defence.

5 Prioritisation of validation resources

Firms continue to seek the optimal balance of frequency and depth for their independent model validations; this activity can be particularly labour-intensive and, as such, it is often subject to headcount pressures alongside aspirations to automate as far as possible. The expectation is that governance arrangements, accountability structures and management information should support effective board oversight. Internal Audit functions should expect greater scrutiny of governance effectiveness and the quality of challenge around climate-related decisions.

2 Maturity enhancement

Other firms across financial services, including insurers, investment managers and smaller banks, continue to focus on enhancing their frameworks including policy design, model inventory completeness and validation coverage.

4 Inventory systems

Firms are investing in software systems for model inventory and lifecycle management; these centralise information, standardise processes, automate MI production and provide a single source of truth regarding the governance status of an object. Many firms are spending significant time and effort to configure these systems to match their firm-specific governance processes.

“The discipline is undergoing a significant transformation due to the increasing power of generative and agentic AI”

Five things Internal Audit should do

1

The interaction between Model, AI and EUDA Risks

Provide assurance that these often-overlapping risk areas are being managed in an effective and efficient way, with appropriate definitions that reflect the true nature of these features and governance processes that are suitably integrated.

2

Independent model validation coverage and effectiveness

Assess the design and operating effectiveness of the independent model validation control, in the context of supervisory expectations, wider industry practice and firms' specific appetite for model risk.

3

Model inventory design

Assess the integrity of the model inventory system, including whether functional coverage is appropriate and the data populated meets the minimum required for governance and compliance processes.

4

Framework enhancement programmes

Whether a large bank with an SS1/23 remediation plan or a smaller firm looking to enhance maturity, assess the design and operating effectiveness of risk transformation programme controls including activity planning, remediation timescales and end-state policy design.

5

Overlap with data governance

Given that issues relating to data inputs are one of the main sources of risk for live models, assess the maturity of the interface between model governance and data governance frameworks and processes, including data ownership, issue identification/management and data quality monitoring.

Operational resilience: from implementation to proof

Operational resilience remains a key board and regulatory priority as firms face increasing disruption from cyber incidents, technology failures, third-party dependencies and operational change. The focus has shifted from traditional business continuity towards ensuring firms can continue delivering important business services within defined impact tolerances during severe disruption.

For UK financial services firms, operational resilience is now an ongoing supervisory expectation. The PRA and FCA's new incident and third-party reporting requirements, effective from 18 March 2027, together with the IIA's Organisational Resilience Topical Requirement effective from 30 April 2027, are raising expectations for governance, testing and assurance. Internal Audit plays a critical role in assessing whether resilience capabilities are embedded, effectively governed and operating as intended across areas including change, third-party management, incident response and crisis management.

1 The regulatory focus moves from Implementation to sustained proof

The operational resilience transition period ended on 31 March 2025, and firms are now expected to demonstrate that important business services can remain within impact tolerances under severe but plausible disruption. The FCA's 2026 observations emphasise that firms should review and evolve their resilience approach using self-assessment insights, including important business services, impact tolerances, mapping, scenario testing, vulnerability management, and governance.

3 Minimum Viable Company, dependency mapping and resilience testing

In parallel, there is growing emphasis on defining the Minimum Viable Company (MVC) — the minimum technology, people, processes and third-party services required to sustain critical operations during disruption. This is driving greater focus on dependency mapping, recovery capability and resilience testing, enabling organisations to identify vulnerabilities and validate whether critical services can continue to operate under adverse conditions.

5 The IIA Organisational Resilience Topical Requirement raises the bar

The IIA's Organisational Resilience Topical Requirement defines a consistent, comprehensive approach and minimum baseline for assessing the design and implementation of organisational resilience governance, risk management and control processes. It also defines organisational resilience as the ability to anticipate, absorb and adapt to disruption, which broadens the focus from continuity and recovery to strategic adaptability and sustained delivery.

2 Operational resilience is than technology resilience

Technology modernisation, cyber recovery, cloud dependency, automation, AI and technology supply chain risk remain important considerations to build technology resilience. Operational resilience, more broadly, requires audit coverage across people, processes, premises, data, technology, third parties, communications, governance, financial resources and customer outcomes.

4 Incident reporting expectations becoming more standardised and data-driven

The FCA's PS26/2: Operational incident and third-party reporting asserts that operational incident reporting rules will define operational incidents, set thresholds, introduce a standardised reporting process and require firms to submit standard or enhanced incident reports. The PRA's SS1/26 – Operational resilience: Incident reporting was published on 18 March 2026 and is effective from 18 March 2027; it applies to UK banks, building societies, PRA-designated investment firms, UK branches of overseas banks, and UK Solvency II firms.

Five things Internal Audit should do

1 Assess whether operational resilience is embedded by design

Review whether operational resilience is owned at board and executive level, supported by clear accountability, risk appetite, metrics, reporting and investment decisions. Assess whether resilience considerations are embedded into strategic planning, product design, transformation, outsourcing, change delivery and technology architecture.

2 Understand what is truly critical

Assess whether management understands and has defined the minimum technology, people, processes and third parties required to sustain critical operations during disruption. Evaluate the organisation's process for substantiating its minimum requirements, including its consideration of service tolerances and critical dependency mapping.

3 Review cyber recovery and recoverability

Consider whether critical services can be recovered following a cyber event, including the effectiveness of backup, restoration and recovery testing arrangements. Assess whether organisations have considered scenarios and testing to address cyber risks associated with the integration of information technology (IT) and operational technology (OT) systems.

4 Assess technology dependency and concentration risk

Evaluate management's understanding of dependencies across cloud providers, technology vendors, data centres and other critical suppliers. Consider additional dependencies on automation and AI, and how management incorporates the use of such technologies into its critical dependency mapping.

5 Challenge resilience testing and continuous assurance

Assess whether testing is sufficiently realistic and whether lessons learned are used to strengthen resilience capabilities over time. Evaluate management's processes for maintaining effective resilience through continuous monitoring and improvement activities.

14 Data quality, MI and regulatory reporting – rising in importance

Overview

Data continues to be a critical focus for Internal Audit functions. Let's not forget, data quality is a fundamental prerequisite for any cost-effective and successful AI implementations. Data remains a core component of numerous audit programmes, reflecting its foundational importance across organisational operations and strategic initiatives. The increasing volume, complexity, and regulatory scrutiny of data necessitate robust oversight, making it an enduring priority for assurance providers in 2027.

Across both the FCA and PRA agendas, there is a very clear message: as supervision becomes more digital, more analytical and more continuous, poor data becomes a bigger regulatory risk. The FCA is building a more data-led supervisory model and digitising more of its interaction with firms. The PRA continues to identify data risk as a core theme underpinning prudential soundness, decision-making and resilience.

Five things you should know about the topic

1 Data as a supervisory priority and AI enabler

Organisations must recognise the critical importance of data, not only as a top supervisory priority for regulators across all sectors and jurisdictions, but also as the foundational enabler for advanced technologies such as Artificial Intelligence. Without robust data integrity, the promise of AI cannot be fully realised, making data a strategic imperative.

3 Data governance, analytics and reporting controls

Firstly, data governance is paramount, as organisations grapple with ensuring data quality, integrity, and effective management throughout its lifecycle. Secondly, data analytics and reporting controls are crucial, given the reliance on data for strategic decision-making and performance measurement, requiring assurance over the accuracy and reliability of insights derived.

5 Automation, AI and data quality assurance

In an era defined by exponential data growth and the rapid adoption of AI and emerging technologies, the traditional reliance on manual data controls and mapping is no longer sustainable or scalable. Internal Audit functions must recognise that future-proofing data controls necessitate a shift towards automation, with AI as a key enabler. It is no longer feasible to deploy full teams for manual data mapping and control enforcement. However, automation must not outpace data quality assurance, as AI trained on poor data, scales and repeats errors.

2 Sustained significance of data within Internal Audit plans

Internal Audit functions highlight the sustained significance of Data within Internal Audit plans – a focus echoed externally by Gartner, whose survey on strategic priorities for CAEs in 2026 found 94% of CAEs planning data governance activity. This consistent focus highlights the pervasive impact of data across all business functions and its inherent risks. The primary drivers influencing this selection are multifaceted.

4 Data regulatory compliance

Data regulatory compliance remains a significant concern, with evolving privacy laws (e.g., GDPR, CCPA) and industry-specific regulations demanding rigorous controls and continuous monitoring of AI use, cross-border data flows, and data sharing, to mitigate legal and reputational risks. These drivers collectively position data as an indispensable area for Internal Audit scrutiny.

“As supervision becomes more digital, more analytical and more continuous, poor data becomes a bigger regulatory risk”

Five things Internal Audit should do

1 Understand data's role in AI and emerging technologies

As firms embark on strategic AI scaling programmes, Internal Audit should assess data quality, provenance, lineage, and fitness-for-purpose controls, together with applicable AI-transparency, privacy, and sector-specific requirements. Testing should evidence how data is collected, processed, governed, and used in AI systems, including controls addressing bias, access, retention, and accountability.

2 Ensure data quality for operational and regulatory needs

Internal Audit should conduct holistic reviews of data quality, recognising its critical impact on both operational efficiency and regulatory reporting. With increasing reliance on data for strategic decisions, audit functions must assess the controls around data analytics processes, from data sourcing and transformation to reporting. This ensures the accuracy, completeness, and reliability of insights used by management.

3 Assess data governance frameworks

Internal Audit should evaluate the maturity and effectiveness of the organisation's data governance framework, including policies, standards, roles, and responsibilities for data ownership, quality, and lifecycle management. This includes ensuring clear accountability for data assets and a unified metadata / data-lineage capability to evidence where AI training data originated.

4 Monitor data regulatory compliance

Monitor applicable data-protection, AI, and sector-specific regulatory requirements, recognising that obligations and effective dates vary by jurisdiction, system type, and organisational role. Assess the organisation's compliance posture, including data handling, lawful basis and consent, data-subject rights, retention, cross-border transfers, and breach-response protocols.

5 Evaluate data security and privacy controls

Beyond governance, Internal Audit needs to scrutinise technical and organisational controls protecting sensitive data from unauthorised access, use, disclosure, disruption, modification, or destruction, including data used by AI systems and agents. This includes data encryption, access management, data loss prevention measures, data classification, and lineage controls.

Cyber security remains the defining technology risk for organisations in FY27, as the threat landscape becomes more complex, automated and interconnected. The rapid adoption of AI, the continued reliance on cloud services and expanding third-party ecosystems are increasing the scale and speed at which cyber risks can affect critical operations, sensitive data and customer trust. Developments of advanced AI models have highlighted the potential for AI to identify and exploit vulnerabilities at unprecedented speed, reducing organisations' ability to rely solely on traditional prevention and patching approaches. With ransomware, identity compromise and supply chain incidents continuing to test organisational resilience, cyber security remains a key area of focus for Internal Audit in assessing whether organisations are prepared to prevent, detect, respond to and recover from cyber disruption.

1 Cyber security remains a key Internal Audit priority theme

Cyber security remains on top of the plan and agendas across FS Internal Audit functions, reconfirming its role as a core assurance priority. Many Internal Audit functions also use data analytics, continuous monitoring and AI-powered tools to assist in those planned audits, and we see their use increasing in 2027. In parallel, organisations are embedding AI into business processes, increasing the need for assurance over data security and protection, secure configuration, access control and governance of AI-enabled systems.

3 Identity, access and recovery remain significant focus areas

Identity and Access Management is a significant focus area, reflecting the prevalence of identity-based attacks and the need for robust controls over privileged access, multi-factor authentication, non-human identities and joiner-mover-leaver processes. Threat detection, incident response and recovery capabilities remain equally important, as organisations need to demonstrate that cyber incidents can be identified, contained and recovered from, before material operational, financial or reputational impact occurs.

“AI-enabled attacks (e.g., Mythos) and the pace of AI-powered vulnerability discovery, have turned the topic into a board level concern”

2 AI-enabled cyber threats are growing in scale, speed and sophistication

AI-enabled attacks (e.g., Mythos) and the pace of AI-powered vulnerability discovery, have turned the topic into a board level concern. Such threats include the use of generative AI to create more convincing phishing campaigns, automate reconnaissance, accelerate malware development and support social engineering.

4 Cyber assurance is becoming more resilience-focused

Collectively, the growth in AI-enabled threats, increasing reliance on cloud and third-party ecosystems, identity-based attacks, heightened regulatory expectations, and the need for effective incident response and recovery capabilities are driving a more resilience-led cyber assurance agenda, covering prevention, detection, response and recovery across the full cyber control environment.

5 Board-level agenda topic

Cyber security is a board level issue. The organisation's risk exposure and profile against the (ever evolving) threat environment should be discussed frequently. In relation to vulnerability posture and remediation strategies, functions should continue the dialogue with cyber leadership, the board and regulators, given heightened expectations for rapid disclosure and accountability. By focusing on these areas, they can help ensure that organisations are not only keeping pace with AI-accelerated threats but are also building resilient, business-aligned cyber risk management foundations.

Five things Internal Audit should do

1 Strengthen cyber governance, regulatory oversight and Board reporting

Internal Audit should assess whether cyber security governance aligns to risk appetite, regulatory obligations, critical services and recognised good practice, including relevant National Cyber Security Centre (NCSC) guidance for the UK, such as the Cyber Assessment Framework, or National Institute of Standards and Technology (NIST) guidance for the US. This should include Board oversight, cyber risk metrics, accountability, investment priorities and reporting on threat exposure and control effectiveness.

2 Prioritise identity and access management assurance

Identity remains a primary route for cyber compromise. Internal Audit should review privileged access, multi-factor authentication, joiner-mover-leaver controls, access reviews and controls over service accounts, machine (agent) identities and other non-human identities. Leverage the function's AI-powered capability to optimise the efficiency and coverage of the audit.

3 AI-driven vulnerability management

AI-driven vulnerability discovery is accelerating the volume and pace of vulnerability identification. Internal Audit should assess whether organisations can rapidly identify, prioritise and remediate vulnerabilities through effective asset visibility, risk-based decision-making, robust escalation processes, compensating controls and secure-by-design development practices. Compensating controls, such as segmentation, and boundary hardening should be in place for systems that cannot be patched quickly.

4 Review third-party, cloud and supply chain cyber risk

Internal Audit should assess whether cyber risks from cloud platforms, Software-as-a-Service (SaaS) providers, managed service providers, critical vendors and outsourced services are understood and managed through secure configuration, vendor assurance, contractual requirements, supplier monitoring and resilience of key dependencies.

5 Embed secure by design, DevSecOps and AI security assurance

Internal Audit should assess whether security is embedded throughout technology change and operations, including AI-enabled solutions. This should include Secure by Design practices, application security, vulnerability management, data protection and access controls. Security should be integrated into development pipelines as a continuous, native step. Audits should also consider AI-specific risks, including model security, data provenance, third-party AI dependencies and governance over the use of emerging technologies.

Transformation & change

Technology and digital transformation remain strategic priorities as organisations invest in cloud migration, system modernisation and AI capabilities to improve customer outcomes, efficiency and competitiveness. While these initiatives create significant opportunities, they also introduce new risks that Internal Audit must understand and address. Increasingly, Internal Audit is expected to provide assurance that transformation programmes are delivering intended business outcomes and value while managing risk effectively.

The rapid advancement of AI is accelerating change and increasing the need for effective governance, portfolio prioritisation, release management and deployment controls. As more technology-enabled change is delivered directly within the business, organisations must ensure transformation activity remains well controlled, aligned to strategic objectives, resilient and focused on customer outcomes.

Digital transformation and value realisation continue to feature prominently in board agendas, risk assessments and Internal Audit plans. Internal Audit should assess whether AI implications have been appropriately considered within business cases, programme design, delivery approaches and performance measures, particularly where initiatives are large, mandatory or regulatory-driven.

1 Economic uncertainty, geopolitical uncertainty and technology-enabled operating models

Economic uncertainty and challenging markets continue to drive initiatives to optimise core operating costs, open new channels or seek strategic restructure whilst remaining compliant with evolving regulation. These changes trigger the critical need for new systems, processes and target operating models that are enabled by digital technology at the core, not as a bolt on to an existing service or way of working.

3 Business-led change and transformation control

Where technology enables increasing amounts of change to be delivered in the business, without the traditional structures of IT functions and change professionals, it is imperative that management, risk and Internal Audit ensure that transformation activity is well controlled, considers the impact on customers appropriately and is aligned to strategic outcomes, while also maintaining operational resilience during periods of significant change.

2 AI agents and governance over change delivery

The rapid change in technology capability driven by AI agents reinforces the need for strong governance over short term portfolio prioritisation, seamless release management and functional deployment controls.

4 Internal Audit's own digital evolution

Internal Audit also needs to transform and not only audit and advise the business on digital transformation. This means integrating GRC systems, adopting new ways of working and embedding AI across the audit lifecycle. By experiencing this transformation first-hand, Internal Audit will be better positioned to act as a trusted adviser.

5 AI-driven dynamic transformation portfolio and business-case reassessment

Rapid advances in AI can materially change the assumptions driving transformation programmes, including solution design, delivery approach, cost, workforce requirements and anticipated benefits. Organisations should establish clear triggers for reassessing business cases and portfolio priorities, including whether programmes should be accelerated, redesigned, paused or stopped. Internal Audit should consider whether these decisions are supported by reliable information, transparent governance and effective tracking of benefits, dependencies and investment.

Five things Internal Audit should do

1

Controls and governance are playing catchup

Teams are under pressure to launch new products and digital capabilities quickly. Rapid prototypes and proofs of concept may be deployed before ownership, accountability and risk assessment are clearly defined. Internal Audit should assess governance pathways from ideation through implementation and ongoing operation, including monitoring temporary workarounds. In doing so, IA teams should be helping the business to identify opportunities to streamline governance – allowing the business and IT teams to focus more on their core responsibilities.

2

Agentic development and vibe coding

Speed outpaces safeguards – Generative AI tools are transforming software development, enabling amateurs to build solutions unsupported. Changes may bypass existing controls and produce limited documentation. Internal Audit should assess whether agentic coding is governed through the software development lifecycle, including access to confidential data, code review, testing, deployment and monitoring controls.

3

Value-focussed scaled Agile

Industries are evolving established waterfall and agile frameworks towards custom value stream models with selected elements of DevOps, Lean and Scrum. Auditing against the framework is not sufficient, and auditors must consider how governance structures are tailored, particularly around scope control and benefits delivery.

4

Trust is not a control

The growing use of open-source datasets and AI models within transformation journeys challenges how organisations map dependencies, trust outputs, and prove sources and test models are representative. Complex dependencies need strong security validation. Internal Audit should consider whether digital trust roles and specialist assurance support are in place for features built on digital supply chains beyond the enterprise.

5

Integrated change assurance

With increasingly rapid change cycles, IA must align change controls assurance across three lines of defence, enabling earlier identification of high-risk areas and jointly driving ongoing intervention across complex change portfolios. Early assurance can help improve programme outcomes, reduce delivery risk and prevent costly remediation by identifying control, governance and delivery issues before they become embedded.

Banking and capital markets and investment management

03



Remuneration remains a critical area of regulatory focus across UK financial services firms, reflecting a continued emphasis on aligning reward, accountability and prudent risk-taking. Regulators have sought to simplify the framework and improve proportionality, while maintaining strong governance over remuneration decisions and preserving the links between variable remuneration and performance, conduct and risk outcomes.

1 Banking reforms reshape variable pay and MRT governance

Following the PRA and FCA's remuneration reforms which took effect in October 2025, banking sector firms have been implementing material changes to their variable pay structures, including in relation to deferral and retention periods, on both an "in-year" and, in some cases, retrospective basis. Firms have also been revising their Material Risk Taker (MRT) identification methodologies to align with the recent changes and the enhanced governance expectations relating to this, including in relation to the role of the Chief Risk Officer. Firms also need to ensure that their assessment of the performance of Senior Managers and the assessment of ex ante risk align with the new rules and guidance provisions.

3 Accountability remains central as SM&CR evolves

The broader regulatory environment is also evolving. Ongoing reforms to the Senior Managers and Certification Regime (SM&CR) – effective September 2026 with further reforms expected to be consulted upon in late 2026 – are intended to reduce administrative burdens while preserving individual accountability. As regulators continue to place great emphasis on conduct, culture and senior manager accountability, firms will need to demonstrate how remuneration outcomes reflect performance against regulatory responsibilities, risk management objectives and the delivery of sustainable business outcomes. Remuneration Committees will be expected to evidence robust challenge, effective oversight and clear links between risk events and pay decisions.

2 A simpler regime brings new complexity for solo-regulated firms

At the same time, the FCA is consulting on substantial reforms to remuneration requirements for solo-regulated firms, including asset managers, wealth managers and investment firms. These proposals are expected to apply from Q1 2027 and result in a simpler and more proportionate regime under a single ruleset, with firms needing to comply with revised requirements for identifying MRTs and key remuneration principles, while demonstrating effective governance over compensation arrangements. Firms operating across multiple regulatory regimes may face increased complexity as UK requirements continue to diverge from EU remuneration rules and expectations.

4 Weak controls can undermine credible pay outcomes

Effective remuneration frameworks depend on robust governance, consistent implementation of regulatory requirements and credible risk adjustment methodologies, particularly for the assessment of future or "ex ante" risks. Weaknesses in the controls supporting remuneration decisions can attract increased regulatory scrutiny, especially where pay outcomes appear inconsistent with financial performance, customer outcomes, risk events or conduct expectations.

"Firms operating across multiple regulatory regimes may face increased complexity as UK requirements continue to diverge from EU remuneration rules"

Five things Internal Audit should do

1 Review implementation of remuneration reforms (for banking sector firms)

Assess the firm's implementation of the PRA and FCA remuneration reforms, including changes to MRT identification, deferral arrangements, retention periods and variable pay structures. Assess whether performance assessments for senior managers adequately consider accountability for regulatory responsibilities, remediation activities, risk management effectiveness and regulatory interactions. Challenge management's interpretation of regulatory requirements.

2 Assess remuneration governance effectiveness

Evaluate the effectiveness of Remuneration Committee governance, including evidence of challenge, decision-making, management information and oversight of remuneration outcomes across the business.

3 Test links between risk, conduct and reward

Review whether variable remuneration decisions at both a bonus pool and individual level appropriately reflect risk outcomes, individual conduct rule breaches, audit findings, regulatory issues and customer outcomes. Assess the operation of the firm's risk adjustment methodology, including the application of any individual risk adjustments.

4 Evaluate the role of control and corporate functions in the remuneration framework

Evaluate the nature of the input provided by the Risk and Compliance functions in the remuneration framework, including in relation to the identification of MRTs and risk adjustment at a bonus pool and individual level. Evaluate the role of the Finance function in the assessment of firm and business unit performance.

5 Review remuneration framework consistency across jurisdictions

For firms operating internationally, assess how differing UK, EU and local remuneration requirements are identified, monitored and applied. Evaluate controls designed to manage regulatory divergence and maintain consistent governance standards.

Private credit is reshaping business finance and the transmission of risk across the financial system. Rapid growth, new fund structures and deeper links between asset managers, banks, insurers and private equity have expanded funding options, but also increased opacity and interconnection. Judgement-led valuations, leveraged borrowers and limited data can delay recognition of stress. As supervisory scrutiny intensifies, internal audit should assess whether governance, risk management, data and liquidity arrangements have kept pace—and whether firms can withstand a prolonged downturn.

The complexity of private credit is driving greater scrutiny, including the Bank of England's system-wide stress exercise for private markets. While some firms are strengthening their own controls ahead of formal requirements, others have yet to invest sufficiently in the processes, data and infrastructure needed to demonstrate resilience—an important area for internal audit challenge.

1 Rapid growth is reshaping the risk landscape

Private credit is expanding beyond direct lending into asset-based finance, special situations, mezzanine and venture debt. Larger transactions and bank-asset manager partnerships are blurring market boundaries. Common borrowers, sponsors, collateral pools, funds and securitisation vehicles can connect exposures, while legal-entity or counterparty reporting may obscure concentrations across products and countries.

3 Opacity is increasing valuation and oversight risk

Bespoke terms, limited comparables and model-based valuations can produce stale or inconsistent marks. Data gaps at borrower, loan and fund level can also obscure leverage and emerging risks. Reported leverage on some deals is around 5–6 times debt to EBITDA, but aggressive add-backs may mean underlying leverage is materially higher.

5 Deepening connections can amplify stress and conflicts

Links between asset managers, banks, insurers, pension funds and private equity sponsors create layers of leverage and channels for contagion. Significant Risk Transfer (SRT) illustrates the issue: a bank may fund a private credit vehicle through subscription or NAV lending while that vehicle provides protection on the bank's SRT. This can diversify risk, but also create circular exposures, related-party conflicts and hidden concentrations that require coordinated oversight.

2 Borrower vulnerabilities are becoming harder to identify

Many borrowers are unrated, highly leveraged and concentrated in sectors such as technology, healthcare and business services. EBITDA adjustments, payment-in-kind interest, covenant resets and restructurings can mask weakening cash flow. Bespoke structures and limited default history also increase reliance on judgement in underwriting, risk ratings and monitoring.

4 New fund structures are increasing liquidity risk

Closed-end funds generally match illiquid assets with stable capital, but semi-liquid and evergreen vehicles offer periodic withdrawals while holding long-dated loans. Growing retail and wealth participation increases the need for realistic liquidity assumptions, transparent investor communications and credible stress-management plans.

“While some firms are strengthening their own controls ahead of formal requirements, others have yet to invest sufficiently in the processes, data and infrastructure”

Five things Internal Audit should do

1 Aggregate exposures and identify hidden concentrations

Assess whether management can aggregate exposures across products, entities and counterparties, including common borrowers, sponsors, collateral pools, funds and securitisation vehicles. Confirm that concentrations and interconnected risks are identified, owned, limited and reported.

2 Identify borrower stress early

Evaluate underwriting standards and private credit scorecards, including borrower cash flow, collateral, loan terms, EBITDA adjustments and sponsor support. Confirm monitoring identifies rising debt, payment-in-kind interest, covenant breaches, restructurings and sector stress early enough for action.

3 Challenge opaque valuations and data gaps

Review whether valuation methods, assumptions and data are reasonable, independently challenged and refreshed when conditions change. Test whether borrower-, loan- and fund-level information provides a reliable view of performance, leverage, covenant headroom and concentrations.

4 Test resilience to liquidity stress

Assess whether asset liquidity, fund terms and withdrawal rights are aligned. Review stress tests covering defaults, valuation falls, redemptions and funding pressure. For semi-liquid and evergreen vehicles, test redemption gates and side pockets, and verify that contingency plans have been exercised rather than merely documented.

5 Assess interconnected exposures and conflicts

Evaluate links with banks, insurers, private equity sponsors and other partners, including indirect exposures and leverage. Review related-party transactions, conflicts, limits and Board reporting. Bank internal audit functions should use the firm's own SRT or synthetic securitisation programme as a specific test case for interconnection risk.

Banking and capital markets and insurance

04

SECTOR BACKGROUND

Prudential risk

As firms plan for 2027, prudential regulation will remain a significant driver of Internal Audit priorities. Banks must prepare for the implementation of Basel 3.1 and the simplified regime for Small Domestic Deposit Takers (SDDTs)—firms with predominantly domestic, relatively simple business models that operate within prescribed prudential thresholds and opt into the regime through a PRA modification by consent—alongside continued supervisory focus on liquidity, structural interest rate risk, regulatory reporting and data quality.

Across the insurance sector, attention remains on underwriting and reserving discipline, financial resilience and the ability to respond effectively to severe but plausible stress events. Internal Audit should assess whether implementation programmes, data and reporting controls, and wider risk and control frameworks are keeping pace with regulatory expectations and business change.

1 Capital regime implementation

Basel 3.1 takes effect on 1 January 2027, changing credit, operational and market risk requirements, with the first returns due in mid-May. SDDT firms will apply the Basel 3.1 Pillar 1 framework with targeted simplifications, including exemptions from due diligence, counterparty credit risk and credit valuation adjustment requirements.

3 Regulatory reporting and data

Supervisory focus is likely to intensify as firms submit their first returns under the new capital regime. Complex IT landscapes, poor data lineage and weak controls can undermine the accuracy and reliability of reporting.

5 Risk governance and control effectiveness

Firms are rationalising control inventories, strengthening risk-to-control linkages, clarifying responsibilities across the three lines and improving independent control testing where frameworks have not kept pace with growth and change.

2 Liquidity and interest rate risk

Firms need a clearer understanding of short-term liquidity risk, appropriate liquid-asset buffers and credible monetisation capabilities. Continued use of fixed-rate instruments and derivatives also places focus on structural hedging and assumptions for the behavioural life of liabilities.

4 Underwriting, reserving and stress resilience

A softening general insurance market may place pressure on pricing, reserving assumptions and underwriting discipline. DyGIST also increases scrutiny of how insurers respond to severe but plausible events, including governance, management information, escalation, decision-making and operational response.

“Complex IT landscapes, poor data lineage and weak controls can undermine the accuracy and reliability of reporting”

Five things Internal Audit should do

1

Capital regime implementation

Review implementation of Basel 3.1 or the SDDT regime, including Pillar 1 assumptions, Pillar 2 assessments, capital impacts, regulatory reporting changes and plans to close compliance gaps. Confirm that new data items can be sourced accurately and that tactical solutions are appropriately governed.

2

Liquidity and interest rate risk

Assess short-term liquidity risk, liquid-asset composition and the firm’s operational ability to access central bank facilities or monetise assets under stress. Review structural hedging, including liability eligibility, deposit behaviour, hedge size and duration, and associated governance.

3

Regulatory reporting and data

Review the end-to-end reporting process, focusing on source data reliability, data lineage and hand-offs between systems and applications. Confirm that manual processes and legacy systems are well controlled and that plans for greater automation are credible.

4

Underwriting, reserving and stress resilience

Evaluate whether pricing, reserving and underwriting controls remain effective as competition increases. Assess governance, management information, escalation and decision-making during stress events, including preparedness for DyGIST and incorporation of relevant lessons into stress-testing, crisis management and resilience frameworks.

5

Risk governance and control effectiveness

Assess control rationalisation, risk-to-control linkage, documentation quality and accountability across the three lines. Evaluate whether independent testing provides timely and reliable assurance over key controls.

Banking and capital markets

05

VECTOR BACKGROUND

Consumer credit regulation and Consumer Credit Act (CCA) reform

On 11 February 2026, the FCA published its final Policy Statement (PS26/1) for providers of Deferred Payment Credit (DPC), commonly referred to as unregulated Buy Now Pay Later (BNPL) products and services. These rules brought previously unregulated BNPL products into the regulatory perimeter from 15 July 2026 (“Regulation Day”).

This represents a significant change in expectations for BNPL firms, requiring previously unauthorised providers to obtain FCA authorisation and firms to design, implement and embed changes to policies, processes, systems and controls within short timescales. Alongside this immediate implementation challenge, wider reform of the Consumer Credit Act 1974 (CCA) is expected to move the consumer credit regime away from detailed statutory prescription towards a more flexible, FCA-led framework focused on clearer information, customer understanding and good consumer outcomes.

1 Consumer Duty

The full scope of the Duty now applies to BNPL firms and the range and depth of requirements poses a significant challenge. In particular, the need for firms to evidence compliance with the Duty will require appropriate monitoring of outcomes – for previously unregulated firms this will likely require significant investment.

3 Arrears management and complaint handling

BNPL firms must communicate with customers about missed repayments, provide reasonable notice before enforcing or terminating an agreement, and signpost free and impartial money guidance and debt advice where customers are in arrears. FCA complaint-handling rules also apply, enabling customers to refer complaints about regulated BNPL agreements entered into on or after Regulation Day to the Financial Ombudsman Service (FOS).

“The full scope of the Duty now applies to BNPL firms and the range and depth of requirements poses a significant challenge”

2 Information requirements

BNPL firms must proactively provide customers with key information before entering into a DPC agreement, including withdrawal and cancellation rights, the consequences of missed payments, and how to complain to the Financial Ombudsman Service (FOS). Although less prescriptive than CONC 4.2, this represents a significant increase in the information previously required.

4 Affordability and Creditworthiness

BNPL firms are now subject to CONC 5.2A affordability and creditworthiness rules, even for agreements under £50. While an exception exists for customers with no obvious material affordability risk, firms must clearly evidence their rationale for using the exception.

5 CCA reform

HM Treasury’s May 2026 Policy Statement signals a significant move away from statutory prescription towards a more flexible, FCA-led regime focused on clearer information, customer understanding and good outcomes. Final legislation and detailed FCA rules are still to follow, giving firms an opportunity to identify friction points and understand the processes, documentation and systems that may be affected.

Three things Internal Audit should do

1

Assurance over the implementation of BNPL regulation

IA should provide assurance over the appropriateness of actions taken and governance applied to demonstrate readiness for implementing BNPL regulation.

This may include assurance over the robustness of the firm’s regulatory gap analysis capturing FCA requirements for BNPL products, the firm’s implementation plans, and associated programme governance arrangements.

2

Post implementation assurance and embedding of BNPL actions across the customer journey

IA should consider performing post implementation reviews to provide assurance as to whether the actions taken as part of BNPL implementation have been sufficiently embedded, align to regulatory requirements, expectations and support the delivery of good customer outcomes.

This could be achieved through targeted design and operating effectiveness reviews across critical components of the BNPL customer journey, including (but not limited to):

- Financial Promotions
- Pre-contract Credit Information and Credit reporting
- Affordability and Creditworthiness
- Treatment of customers in Financial Difficulty (including Vulnerable Customers)
- Debt Disputes
- Complaints
- Consumer Duty Rules and Requirements.
- Governance, MI and monitoring arrangements

3

Prepare for CCA reform

IA should monitor developments and engage with relevant business areas as they prepare for consultation, sharing insights from previous reviews, control observations and actions relating to CCA friction points. IA should also assess whether affected customer journeys, processes, documentation and systems have been mapped sufficiently to support informed engagement with the FCA.

Conduct risk and non-financial misconduct

Conduct risk remains a core financial-services concern. Weak governance, incentives, product design and challenge can cause customer harm, market-integrity failures and enforcement. It concerns whether firms deliver appropriate outcomes for customers, clients, employees and markets—not simply rule compliance. From 1 September 2026, the FCA's revised non-financial misconduct framework strengthens expectations for workplace behaviour, fitness and propriety and accountability. Internal Audit should assess whether conduct is embedded across strategy, culture, products, distribution, operations and people processes, supported by reliable data and escalation. For retail businesses, this includes the Consumer Duty; the separate Customer Outcomes topic covers Duty governance, monitoring and board reporting.

1 Conduct supervision is increasingly becoming outcomes-focused and connected to Customer Duty

Firms must demonstrate that governance, products, services and controls deliver appropriate outcomes, not rely on compliance. For retail businesses, the Consumer Duty is central to preventing foreseeable harm. Conduct risk also covers wholesale markets, employee behaviour, culture and non-financial misconduct. Regulatory simplification increases management accountability, requiring dynamic audit planning and integrated assurance as rules or business models change. Wholesale and capital-markets surveillance should be proportionate to products, venues, strategies and client activity.

3 Non-financial misconduct is part of the wider culture and accountability framework

From 1 September 2026, the FCA's new rule extends Conduct Rules coverage in non-bank firms to specified work-related bullying, harassment and violence with a sufficient workplace connection. It primarily affects Senior Managers, Certified Persons and Material Risk Takers in firms subject to the regime.

Guidance covers managers' reasonable steps, fitness and propriety, private-life boundaries, social media and unproven allegations. Conduct Rules assessments focus on work-related behaviour; Fitness & Propriety may consider wider matters, subject to legal, privacy and employment constraints. The rules are not retrospective and firms need not proactively monitor private lives or social media.

2 Sector-specific manifestations of conduct risk remain significant

Banking and lending risks include affordability, vulnerable-customer treatment, sales, servicing and redress. Insurance priorities include claims, premium finance, product governance, remuneration, price and value. Investment and wealth-management risks include suitability, ongoing advice, private-market valuation conflicts, fees and service delivery.

4 Data is essential to evidence customer and conduct outcomes

Granular, accurate and timely information is needed to identify outcomes across customer groups, products, channels and third parties. Indicators include complaints, claims, cancellations, declined transactions, pricing, service failures, advice reviews, vulnerable-customer outcomes, employee cases and remediation. Effective surveillance also requires sound data and model governance.

5 Culture, incentives and organisational behaviour connect individual events to systemic risk

Conduct failures may stem from remuneration, sales pressure, management tolerance, weak challenge or fragmented accountability. Conflicts can span sales, trading, research, investment banking, valuation, allocation, personal account dealing and information barriers. Culture reviews should assess behaviour, psychological safety and whether incentives support appropriate customer and employee outcomes. Mature firms may have established investigation and reporting frameworks; others need education, policy and governance enhancements.

Five things Internal Audit should do

1 Assess the enterprise conduct risk framework

Review whether taxonomy, appetite, policies and governance cover risks to customers, clients, markets, policyholders and employees. Test how conduct is embedded in strategy, products, distribution, pricing, claims, advice, servicing, outsourcing, change and remediation. Assess controls including market-abuse and communications surveillance, trade monitoring, escalation, investigations and regulatory reporting.

2 Evaluate outcome monitoring across sectors

Test whether reliable, granular data identifies harm across products, channels, intermediaries and customer cohorts. For insurers, cover claims, premium finance, fair value and distribution; for investment and wealth management, suitability, advice, valuation conflicts, fees and services; and for banking and capital markets, lending, vulnerability, sales practices and market integrity.

3 Review NFM implementation and fitness and propriety

Assess whether work-related and private-life boundaries are clear and decisions consistent across HR, Compliance, Legal and the business. Review personal-data use, investigations, evidence and management information for legal and privacy compliance. Confirm affected staff are trained and escalation pathways understood.

4 Assess culture, incentives and psychological safety

Evaluate whether remuneration, objectives, performance and promotion reinforce appropriate conduct. Use surveys, interviews, whistleblowing and employee-relations data, where lawful, to assess challenge and speaking up. Determine whether management addresses root causes and repeat themes. Review whether boards receive balanced information on surveillance gaps, alerts, conflicts, breaches, investigations and remediation.

5 Provide integrated and forward-looking assurance

Coordinate assurance across Compliance, Risk, HR, Legal, customer-outcomes teams and specialists. Review horizon scanning and change governance, confirm ownership of emerging obligations and use thematic testing to identify systemic weaknesses. Report control exceptions and whether the firm can evidence sustainable, appropriate outcomes.

Preparing for the next phase of payments regulation

Payments firms are entering a period of regulatory and technological change. Although formal adoption and implementation of PSD3/PSR have moved back, some firms are already mobilising programmes and undertaking detailed impact and gap assessments across regulatory requirements, business models, customer journeys, systems, data and controls. Changes to licensing, tokenised payments, fraud prevention and regulatory reporting are also creating complex interdependencies across functions and legal entities. Alongside preparing for evolving regulatory requirements, internal audit functions should maintain a continued focus on the effectiveness of fundamental payments controls.

1 PSD3/ PSR is a 2027 transformation programme

The framework is expected to apply around mid-2028, 21 months after entry into force. Firms should already be completing gap analyses covering fraud liability, verification of payee, strong customer authentication, open banking and fee transparency, with the extended implementation period creating an important window to define scope, dependencies and remediation priorities.

3 Licensing readiness is becoming more evidence-based

Payment institution, e-money and cryptoasset applicants must demonstrate that their operating model, governance, financial resources and controls work in practice, not merely submit documentation. Evidence should map each applicable requirement to an accountable owner and an operating control, for example Board approvals, capital calculations and evidence that CASS safeguarding or custody requirements are met through safeguarded-account records, daily reconciliations, third-party due diligence, resolution packs and, where applicable, asset records and private-key controls.

5 Non-financial risk reporting is becoming broader and interconnected

Requirements cover fraud, complaints, customer outcomes, incidents, service availability, breaches and third parties, with one event potentially triggering multiple reports. From 18 March 2027, new FCA incident and material third-party reporting requirements apply, increasing the need for clearer inventories, ownership, data lineage, thresholds and consistency across submissions and management information.

2 UK cryptoasset authorisation is becoming time-critical

The regime commences on 25 October 2027, with applications open from 30 September 2026 to 28 February 2027; existing registrations and permissions will not convert automatically. Firms will need to complete perimeter assessments, permissions mapping, evidence preparation and contingency planning in advance of the application window.

4 APP fraud is shifting towards prevention and demonstrable customer outcomes

Since October 2024, sending and receiving firms have shared reimbursement costs, with claims generally capped at £85,000. Despite falling losses, outcomes remain inconsistent, and Reporting Standard B is planned for December 2026, increasing the focus on prevention, reimbursement decisions, vulnerable-customer treatment, complaints and reporting.

Five things Internal Audit should do

1

Assure PSD3/PSR readiness

Establish a clear understanding of the firm's current and planned payment products, underlying payment flows and future development plans. Confirm whether the PSD3/PSR gap analysis has started, assess its scope and maturity, and reflect key milestones in the audit universe and forward plan. Once management's assessment is sufficiently developed, review its completeness across affected products, entities, customer journeys, systems and controls, and assess programme governance, resourcing, dependencies and remediation planning ahead of implementation.

2

Assess tokenised-payment and custody controls

Challenge the governance and risk assessment for stablecoins, tokenised deposits and custody services. Review asset backing, redemption, safeguarding, reconciliations, wallet and private-key security, financial-crime controls, customer disclosures, outsourcing, cyber resilience and accountability across payment functions.

3

Provide pre-authorisation assurance over licensing readiness

For payment, e-money or cryptoasset authorisations, assess whether licence and permissions mapping is complete and supported by effective programme governance, ownership and Board oversight. Review application evidence, gap closure and post-authorisation assurance needs, while ensuring management retains ownership of regulatory-perimeter decisions.

4

Evaluate APP fraud controls and customer outcomes

Test end-to-end fraud prevention and reimbursement controls, including confirmation of payee, transaction monitoring, mule-account detection, claims decisions, vulnerable-customer treatment and complaints handling. Use outcomes data to assess reimbursement timeliness and fairness, identify control weaknesses and challenge management's remediation. Assess readiness for Reporting Standard B, and once adopted, test the completeness, accuracy, reconciliation and governance of the compliance data submitted.

5

Assure the end-to-end non-financial risk regulatory reporting framework

Assess whether the firm has a complete inventory of non-financial risk returns, notifications and data requests, with clear ownership, thresholds and data lineage. Review readiness for the FCA's operational incident and material third-party reporting requirements effective from mid-March 2027.

Credit risk remains a key priority for internal audit in 2027. As borrower and counterparty behaviour, technology and macroeconomic conditions evolve, firms must ensure their credit frameworks, models, data and governance remain effective. Internal audit should assess whether firms can identify and respond to risks that could undermine future resilience.

1 Credit growth discipline

Shifting portfolios and rapidly changing processes are testing credit controls. Entering new segments, loosening underwriting standards, streamlining processes or accepting more exceptions can create new risks. Small changes to scorecards, affordability rules or exception handling can alter the portfolio risk profile over time.

3 Credit risk data and MI

Incomplete, inaccurate or untraceable customer, exposure, collateral, arrears or performance data can undermine decisions, reporting and identification of emerging risks or policy breaches. Automation increases reliance on data across systems and providers; weak governance, ownership or lineage can produce unreliable MI and hidden control weaknesses.

5 AI and automation in credit risk

As automation expands across the credit lifecycle, governance may not keep pace with the speed and complexity of decisions. Limited transparency over model logic, data and outcomes can constrain management challenge, increasing the risk of inappropriate lending, poor customer outcomes and weak oversight.

2 Credit model performance, overlays and management judgement

Changing customer behaviour, macroeconomic volatility and sector risk are testing credit models. Pressure within specific portfolios may be difficult to identify, increasing reliance on overlays and judgement. These require clear evidence, independent challenge and outcome monitoring; otherwise, poor judgement can distort model outputs, delay action and overstate resilience.

4 Counterparty credit risk oversight

For firms with material counterparty exposures, volatility, product complexity and interconnectedness can cause risks to build rapidly and remain obscured by fragmented measurement. The PRA continues to focus on exposure methodologies, stress testing, counterparty due diligence, collateral, concentration monitoring and governance. Firms should identify emerging vulnerabilities before they materialise.

“Changing customer behaviour, macroeconomic volatility and sector risk are testing credit models”

Five things Internal Audit should do

1

Credit growth discipline

Assess whether growth plans align with Board-approved risk appetite. Review whether credit policies, underwriting standards and lending criteria remain appropriate for new products and customer segments. Test whether overrides, waivers and policy breaches are identified, challenged and addressed. Assess whether early warning indicators detect deterioration before arrears increase.

2

Models and judgement

Assess modelling controls with relevant SMEs, confirming assumptions remain valid, models operate within defined boundaries and emerging risks are captured. Evaluate whether overlays receive robust independent review in line with SS1/23, address identified weaknesses, have clear ownership and review cycles, and are supported by evidence and defined exit criteria.

3

Credit risk data and MI

Perform independent review and challenge over data governance, architecture, lineage and lifecycle controls, including independent testing of critical data for accuracy, completeness, timeliness, integrity and traceability. Evaluate compliance with BCBS 239 and the scalability of controls. Confirm that management information is reliable, audience-appropriate and sufficient to support decisions and identify emerging risks.

4

Counterparty credit risk oversight

For firms with material counterparty exposures, assess whether frameworks support forward-looking identification, measurement and management of vulnerabilities. Review exposure methodologies, stress testing, due diligence, credit assessment, limit-setting, collateral and concentration monitoring. Test prompt, accurate aggregation across products, counterparties and legal entities to identify concentrations and wrong-way risk, and assess whether governance provides timely, decision-useful insight.

5

AI and automation in credit risk

Ensure automated and AI-enabled credit risk tools are inventoried, risk-classified, and governed effectively. Engage SMEs to confirm that credit decisions are reliable, explainable, and subject to robust oversight. Where applicable, independently test key models and tools against a range of challenger approaches to validate that outputs fall within a plausible spectrum of outcomes.

Insurance

06

24 Pensions reform, consolidation and value for money

Overview

The UK Defined Contribution (DC) pensions market is undergoing significant reform, driven by the Value for Money (VfM) regime, market consolidation, Guided Retirement and Targeted Support. VfM will require schemes to demonstrate value through comparable assessments of investment performance, costs and service quality, while consolidation reforms are mandating fewer, larger schemes with greater scale and investment capability.

At the same time, firms are redesigning retirement propositions and customer journeys. Guided Retirement will need to be offered as the default decumulation solution to disengaged customers while Targeted Support aims to help engaged customers make better retirement decisions.

These reforms will require strategic decision making and challenging implementation in a short space of time. Internal Audit has an important role in assessing whether governance, data, investment decision-making and change programmes remain effective as firms adapt their operating models and customer propositions.

Five things you should know about the topic

1 Implementation of VfM is now the near-term priority

Implementation of the Value for Money (VfM) regime is now a key priority for pension providers. Firms are preparing for phased implementation, with FCA data collection expected to commence from 2027 and the first VfM assessments required for larger schemes in 2028. The regime will require firms to produce prescribed assessments across investment performance, costs and charges, and service quality, with outcomes benchmarked against peers and supported by defined metrics and RAGG (Red, Amber, Light Green, and Dark Green) ratings. This places increased emphasis on the quality of data, reporting, governance and management information needed to evidence performance and support regulatory scrutiny.

3 Consolidation pressure is increasing

The Government's scale agenda is expected to accelerate market consolidation, with providers expected to meet a £25bn scale threshold by 2030. Schemes with more than £10bn in assets may be eligible to apply for a transition pathway where they can demonstrate a credible plan to reach the £25bn threshold by 2035. This is likely to drive strategic decisions around consolidation, acquisitions, growth plans and operating model transformation as firms assess their long-term viability and competitiveness.

2 VfM will reshape investment strategy, not just reporting

Public benchmarking and ratings will create incentives to revisit asset allocation, default design and performance targets. This could improve member outcomes, but also increases the need for disciplined controls over investment decisions, valuation, liquidity, transparency and risk appetite.

4 Product and distribution models are evolving

Firms are increasingly focused on developing new retirement propositions, including Guided Retirement, which is expected to become mandatory from 2028, alongside wider decumulation and Targeted Support offerings. This will require firms to make strategic decisions about product design, customer journeys and how propositions are delivered across digital, workplace and intermediary channels. As innovation accelerates, firms will need robust governance over advice and guidance boundaries, communications, customer segmentation and outcome monitoring

5 Data remains the critical enabler

VfM, pensions dashboards, customer engagement, consolidation and outcome monitoring all depend on complete, accurate and accessible data. Weak data lineage, legacy administration platforms and inconsistent reporting definitions may undermine regulatory readiness and strategic decision-making.

Five things Internal Audit should do

1 Value for Money implementation and consequences

Assess whether governance, data, management information and reporting arrangements are sufficient to support the production of prescribed VfM assessments. Review how management monitors and responds to potential RAGG ratings, including the implications for member outcomes, scheme viability, consolidation risk, growth strategy and the potential closure of underperforming schemes to new members.

2 Investment strategy, performance and control environment

Review how changes to default strategies, asset allocation and performance objectives are governed in response to evolving market and regulatory expectations. Assess controls over investment decision-making, valuations, liquidity, transparency, cost disclosure and risk appetite to ensure firms appropriately manage the risk of excessive risk-taking and performance-chasing while seeking to improve long-term member outcomes.

3 Consolidation strategy and operating model transformation

Review governance over scale plans, mergers, transfers, platform migrations and operating model change. Assess whether decisions are supported by robust analysis of operational resilience, data migration, member impact, cost, execution risk and long-term sustainability.

4 Data, product innovation and customer propositions

Assess whether data governance, reporting controls and customer data frameworks are sufficiently mature to support Value for Money assessments, pensions dashboards and emerging retirement propositions. Review governance over Guided Retirement, Targeted Support and wider decumulation offerings, including product design, customer segmentation, distribution channels, communications, outcome testing and monitoring. Assess whether firms can evidence good customer outcomes, effective conduct risk management and appropriate oversight across an increasingly diverse suite of products and customer journeys.

5 Board oversight, challenge and accountability

Assess whether Boards and committees provide effective oversight of pensions reform, with clear accountability, documented challenge and decisions aligned to Consumer Duty requirements and the objectives of the Government pension reform agenda.

Claims handling and customer outcomes

Claims handling is a critical indicator of customer trust, product value and operational control as insurers' promises are tested. This matters more now as the FCA's scrutiny moves from process compliance to evidence of real customer outcomes, with claims performance, complaints and value measures increasingly used to identify poor value, harm and weak oversight.

For Internal Audit, claims is no longer a narrow operational review: it is a key lens for assessing whether governance, data and accountability are strong enough to detect issues early, challenge management action and support timely remediation.

1 The FCA has intensified its scrutiny of claims handling practices

In 2025, the FCA published findings from its review of home and travel insurers, identifying weaknesses in claims governance, service quality, processes to support vulnerable customers, oversight of outsourced providers and monitoring customer outcomes. The publication signals a shift from claims handling being a routine supervisory topic to an area of enhanced regulatory focus and intervention.

3 Outsourced claims models face increasing challenge

Recent FCA findings highlighted weaknesses in oversight of third-party claims administrators, fulfilment providers and delegated claims arrangements. Further regulatory work is expected to focus on whether firms retain sufficient control and accountability for customer outcomes across outsourced claims activities.

5 Claims data is becoming a primary supervisory lens

FCA General Insurance Value Measures reporting under SUP 16.27 reflects the regulator's increasing expectation that firms use data to build a standardised view of product value and identify emerging customer harm or systemic issues. This includes claims frequency, claims acceptance rates, average claims pay-outs and claims complaints. Firms must evidence that claims, complaints, quality assurance and root cause analysis data are used to challenge poor value indicators and drive timely remediation.

2 Claims handling has become a key Consumer Duty testing ground

Regulators are increasingly using claims outcomes as evidence of whether firms are delivering good customer outcomes and value for money in practice. Claims acceptance rates, complaints, approach to supporting vulnerable customers and settlement approaches are receiving greater scrutiny as indicators of potential customer harm.

4 Storm and weather-related claims have become a conduct risk focus

Industry and regulatory reviews have highlighted cases where customer expectations differed from policy coverage, particularly regarding storm definitions, claim repudiations and the use of cash settlements. Firms need to take on board lessons learned from the storm and weather-related focus area to other claims areas to demonstrate that claims decisions and communications align with customers' reasonable expectations.

“Recent FCA findings highlighted weaknesses in oversight of third-party claims administrators, fulfilment providers and delegated claims arrangements”

Five things Internal Audit should do

- 1 Assess Consumer Duty outcomes across the claims journey**
 Building on the outcome assessment and monitoring areas set out in the Customer Outcomes Topic; evaluate whether management information, governance and outcome testing are operationally effective and therefore can firms evidence that customers receive good outcomes throughout the claims lifecycle, including different customer groups e.g. vulnerable customers.
- 2 Review claims decision-making and customer communications**
 Assess whether claim acceptance, repudiation and settlement decisions are consistent, supported by appropriate evidence and communicated clearly to customers, particularly where coverage interpretations may differ from customer expectations.
- 3 Evaluate oversight of outsourced claims activities**
 Review whether governance and controls over Third Party Administrators ('TPAs'), loss adjusters, fulfilment providers and delegated claims arrangements, including service performance monitoring, quality assurance, customer outcome metrics and escalation processes.
- 4 Assess the effectiveness of claims MI and root cause analysis**
 Evaluate whether claims, complaints and quality assurance data (including root cause analysis) are sufficiently comprehensive to identify emerging risks, customer harm trends and systemic control weaknesses, and whether management takes timely and appropriate corrective action.
- 5 Review resilience of claims operations during surge events**
 Assess whether claims functions can maintain service standards and customer outcomes during periods of elevated claims volumes, including severe weather events, operational disruptions and third-party service provider failures.

Solvent exit planning: from policy compliance to executable readiness

Overview

With the 30 June 2026 implementation deadline for the PRA's solvent exit planning requirements now passed, the focus is shifting from compliance to execution readiness. A solvent exit is the process by which an insurer ceases business in an orderly manner, remaining solvent throughout, without relying on insolvency or resolution measures.

Firms must be able to demonstrate not only that a Solvent Exit Analysis exists, but that governance, triggers, management information, resourcing and contingency actions would support an orderly and solvent exit in practice.

The challenge is increasingly whether solvent exit capabilities are operationally credible, tested and capable of being executed when required.

Five things you should know about the topic

1 The PRA's solvent exit requirements are now entering the embedding phase

Following publication of PS20/24 and SS11/24 in December 2024, insurers were expected to have compliant Solvent Exit Analyses (SEAs) in place by 30 June 2026. The regulatory focus is now shifting from whether firms have developed a plan to whether they can effectively execute it.

3 Solvent exit indicators, triggers and management information are critical

Firms should have defined indicators and escalation thresholds that provide early warning of financial, operational or strategic deterioration. Supporting management information should enable timely decision-making, facilitate Board oversight and provide clarity on when solvent exit options should be considered.

5 Independent assurance is becoming increasingly important

Solvent exit planning is one of the few prudential areas where the PRA explicitly references the need for adequate assurance activities. Firms should be able to demonstrate challenge and validation of assumptions, governance arrangements, trigger frameworks and operational feasibility.

2 Firms must demonstrate credible governance and accountability

The PRA expects firms to establish clear governance arrangements for solvent exit planning, including Board oversight, Senior Manager accountability, documented decision-making responsibilities and escalation processes. Governance should support both business-as-usual monitoring and the activation of solvent exit arrangements should conditions deteriorate.

4 Operational readiness is a growing regulatory focus

The PRA expects firms to understand how a solvent exit would be executed in practice. This includes identifying credible exit options, key operational dependencies, resource requirements, outsourcing arrangements, communication plans and potential barriers to execution. To demonstrate readiness, firms should be able to evidence clear execution plans, defined ownership and governance, realistic timelines, assessment of key dependencies, and processes for managing and escalating execution risks. The focus is increasingly on whether plans can be delivered in practice rather than simply documented.

Five things Internal Audit should do

1

Assess Solvent Exit Analysis (SEA) readiness

Review whether the SEA meets PRA requirements and reflects a realistic assessment of solvent exit options, barriers, assumptions, costs and execution risks.

2

Evaluate governance and trigger frameworks

Assess whether solvent exit indicators, escalation thresholds, management information and decision-making processes are clearly defined, understood, in operation and capable of supporting timely action.

3

Challenge operational executability

Evaluate whether the firm has identified and assessed key operational dependencies, including third-party providers, technology, data, people and contractual obligations that may impede execution.

4

Review stress testing and scenario analysis

Assess whether solvent exit scenarios have been sufficiently tested and whether management understands how changing financial, operational or market conditions could affect feasibility and timing.

5

Exit barriers, contingencies and remediation plans

Review whether the firm has identified key barriers to execution, including legal, operational, funding, outsourcing and regulatory constraints, and established credible contingency actions and remediation plans to address them before solvent exit becomes necessary.

Bulk purchase annuities, funded reinsurance and private market investment strategies

Overview

Improved pension scheme funding levels and a growing number of schemes seeking to transfer pension risks to insurers continue to drive strong demand for Bulk Purchase Annuities (BPAs). At the same time, increasing uncertainty over the future use of funded reinsurance and growing exposure to private credit and other private market assets continue to reshape the BPA sector.

Regulatory scrutiny is now focused on whether firms can maintain pricing discipline, operational capability and robust investment governance as transaction volumes increase and investment strategies become more complex.

In a more competitive BPA market, firms will need to evidence disciplined underwriting, credible capital options, effective oversight of private market exposures and strong customer outcomes through onboarding and ongoing servicing.

Five things you should know about the topic

1 Increasingly competitive market creating pricing risk

BPA volumes are expected to remain strong, with annual transaction volumes projected to reach £45bn-£50bn in 2026. As competition intensifies, the PRA has highlighted the importance of maintaining underwriting discipline and robust pricing controls to ensure firms are appropriately compensated for the risks they assume. Particular focus is being placed on the governance and approval of non-standard transaction clauses, including bespoke contractual provisions and solvency-triggered termination rights.

3 Private credit remains in focus

Life insurers continue to increase allocations to private credit, infrastructure debt, structured finance and other illiquid assets in support of BPA growth and matching adjustment strategies. Regulators increasingly expect firms to demonstrate robust investment governance, appropriate expertise, effective credit assessment processes and clear oversight of valuation methodologies, liquidity risks and conflicts of interest.

2 Funded reinsurance may be less attractive

The PRA's consultation on funded reinsurance (CP8/26) proposes changes that could materially increase the capital requirements associated with certain funded reinsurance arrangements, particularly those involving external counterparties. If implemented, the proposals could reduce the economic attractiveness of funded reinsurance for some BPA providers and increase focus on alternative sources of capital and growth funding.

4 Investment governance expectations continue to evolve

As asset portfolios become increasingly complex, firms are expected to demonstrate that investment committees, Boards and risk functions provide effective oversight and challenge. Regulatory focus is increasingly extending beyond investment performance to encompass risk-adjusted returns, stress testing, asset quality monitoring, concentration risk and the appropriateness of governance arrangements supporting investment decisions.

5 Pension Scheme Trustees are demanding better customer servicing as a differentiator

Trustees increasingly view onboarding quality, member experience and servicing capability as differentiators. Reliance on third-party administrators creates a need for strong oversight, customer outcome monitoring and operational resilience.

“Scrutiny is now focused on whether firms can maintain pricing discipline, operational capability and robust investment governance”

Five things Internal Audit should do

1 BPA pricing, underwriting and non-standard terms

Assess whether pricing, underwriting and transaction approval controls remain disciplined in a more competitive market. Review model governance, challenge over assumptions and controls for bespoke trustee requirements, including non-standard contractual clauses.

2 Capital strategy and funded reinsurance transition

Assess whether management has evaluated the potential impact of the PRA's proposed funded reinsurance reforms on future BPA growth and capital capacity. Review how alternative sources of capital and risk transfer are identified, assessed and approved, including governance arrangements, risk appetite alignment and Board oversight. Consider whether management information supports effective decision-making over growth, profitability, capital deployment and long-term sustainability.

3 Private credit and complex asset oversight

Evaluate governance over private credit, infrastructure debt and other illiquid assets, including due diligence, valuation controls, concentration limits, stress testing and ongoing credit monitoring. Include conflicts of interest where affiliates originate or manage assets.

4 Investment governance and portfolio challenge

Assess whether Boards, investment committees and risk functions provide effective challenge over investment strategy, asset quality, risk-adjusted returns, liquidity and concentration risk. Review whether management information supports timely and informed decision-making.

5 Operational resilience, onboarding and customer outcomes

Review whether onboarding, administration and servicing processes can support continued BPA growth while delivering good customer outcomes. Assess oversight of third-party administrators, operational resilience arrangements, service performance monitoring and management information used to identify and address customer and operational risks.

Investment management and wealth

07

28 Private markets valuation governance

Overview

As investment allocations to private markets continue to grow, governance of illiquid valuations remains a regulatory hot topic. Valuations for private market assets often rely on judgement, models and limited observable data, increasing the need for robust controls and governance to evidence fair, independent and consistent outcomes. The FCA's 2025 private market valuation review highlighted governance, independence, documentation, ad hoc valuations and valuation related conflicts as key areas of focus, while the CSSF's 2026 thematic review reinforced the regulators expectations for robust policies, controls, model oversight, and clear escalation processes when it comes to private markets valuations. Against this backdrop, firms should understand the key valuation governance risks and consider how Internal Audit can provide assurance over the design and operating effectiveness of related controls.

Five things you should know about the topic

1 Judgement-driven valuation risk

Valuation outcomes can be highly sensitive to the selected valuation methodologies and models applied, calibration decisions, unobservable inputs and assumptions, and management judgement. Weak evidence for key assumptions, inconsistent use of comparatives or insufficient challenge over management adjustments can have a significant impact on valuations, impacting performance reporting and investor disclosures.

3 Governance and independent challenge

Regulators expect clear ownership over valuations, functional independence within the process, and effective committee oversight over valuations. Valuation committees should have appropriate authority, expertise and timely information to challenge the valuations and judgements made, approve methodology changes and challenge any exceptions.

5 Stressed markets and ad hoc valuations

Periodic valuation cycles may be insufficient when markets deteriorate, liquidity reduces, observable inputs disappear or assumptions become outdated. Firms should define clear triggers for ad hoc valuations, supported by controls over third-party valuers, model governance and challenge of judgemental inputs and assumptions.

2 Need for appropriate documentation

There are greater expectations on documenting key decisions to evidence the discussions and challenge to demonstrate effective control, not just approval of valuation outcomes.

4 Conflicts of interest

The FCA's ongoing private markets conflicts review is looking into how firms identify, document, escalate and mitigate valuation-related conflicts. This includes valuation conflicts in relation to fees, remuneration, cross-fund transactions, asset transfers, and investor reporting.

“Regulators expect clear ownership over valuations, functional independence within the process, and effective committee oversight over valuations”

Five things Internal Audit should do

1

Judgement-driven valuation risk

Review valuations to confirm that the methodologies, assumptions, inputs and any adjustments are documented and justified, and that they are current, consistently applied and subject to effective challenge. Confirm that judgmental adjustments are clearly evidenced.

2

Governance and independent challenge

Review committee terms of reference, packs and minutes to assess ownership, independence from portfolio management, escalation routes and evidence of challenge over assumptions, methodology changes, exceptions and approvals.

3

Assess the completeness of the documentation

Review the documentation of the key judgements to determine if they are appropriate for the size and risk of valuations.

4

Conflicts of interest

Review conflicts of interest frameworks to evaluate whether valuation related conflicts are identified, documented, escalated and mitigated before valuations are finalised. Assess that these at a minimum cover the potential conflicts identified by the FCA in their 2025 review Private Markets Valuation fees and remuneration, cross-fund transactions, asset transfers, preferential investor treatment and fundraising materials.

5

Stressed markets and ad hoc valuations

Assess whether policies define clear triggers for ad hoc valuations during market disruption, liquidity stress or material assumption changes, and test whether escalation, approval and investor communication processes operate promptly.

29 T+1 settlement and fund settlement transformation

Overview

The transition to T+1 settlement represents one of the most significant operational changes facing firms across the investment ecosystem in recent years. Alongside the move by the UK, EU, and Switzerland to adopt T+1 securities settlement in October 2027, the industry is also progressing towards shorter fund settlement cycles, with a significant proportion of funds expected to move to T+2 settlement. Together, these changes will require firms to redesign operating models, enhance automation, improve data quality, and strengthen post-trade controls across the investment lifecycle.

Five things you should know about the topic

1 The UK, EU and Switzerland are preparing for a move to T+1 securities settlement in October 2027

Following the successful North American transition, industry focus is shifting from impact assessments towards operating model redesign, technology change, testing, and implementation readiness.

3 The transition will expose weaknesses in manual processes and fragmented operating models

Firms with limited straight-through processing, poor data quality or significant reliance on manual intervention may face increased settlement risk, operational exceptions, and resource pressures.

5 Many firms are using the transition as a catalyst for broader operational transformation

Programmes increasingly extend beyond regulatory compliance, encompassing operating model simplification, enhanced automation, improved controls, and more resilient post-trade processes.

2 The transition extends beyond securities settlement

In parallel with the move to T+1, much of the European fund's industry is expected to transition towards T+2 settlement cycles for subscriptions and redemptions. Together, these changes will compress operational timelines across trading, cash management, fund dealing, and investor servicing activities.

4 Data quality and automation will become increasingly important control considerations

Compressed settlement windows reduce the time available to identify and resolve issues, increasing the importance of accurate reference data, automated processing, and effective exception management frameworks.

“These changes will require firms to redesign operating models, enhance automation, improve data quality, and strengthen post-trade controls across the investment lifecycle”

Five things Internal Audit should do

1 Programme governance and third-party readiness

Assess whether management has established an effective governance framework, with clear accountability, escalation routes, and readiness criteria. Particular focus should be given to external dependencies, ensuring critical service providers, market counterparties and technology vendors have been appropriately incorporated into programme plans, risk assessments, and readiness monitoring.

2 Transition testing and market readiness

Review the design and execution of the testing strategy as the industry moves towards market-wide testing in 2027. Internal Audit should assess whether test scenarios are sufficiently comprehensive, covering high-volume periods, late trade activity, funding constraints, cross-border transactions, market disruptions, and end-to-end settlement workflows. Coverage should extend beyond successful processing to include failure, recovery, and contingency scenarios.

3 Exception management

Evaluate whether management has identified the key points where settlement activity could fail and whether controls exist to detect, prioritise, escalate, and resolve exceptions within compressed timelines. Particular attention should be given to unmatched trades, failed settlements, manual interventions, unresolved breaks, and operational dependencies that may become more pronounced under T+1.

4 Liquidity and funding management

Assess whether cash forecasting, FX execution, liquidity management, and settlement funding processes have been redesigned to support compressed settlement timelines. Internal Audit should review potential impacts on liquidity risk, funding arrangements, overdraft facilities, and cash management controls, particularly during periods of market stress or elevated trading volumes.

5 Post-implementation monitoring

Review the metrics, governance and management information established to measure transition success. Internal Audit should assess whether firms are monitoring settlement efficiency, fail rates, exception volumes, liquidity impacts, and root causes, and whether lessons learned are being incorporated into ongoing operating model improvements.

30 Non-financial regulatory reporting – trade & transaction reporting

Overview

Non-Financial Regulatory Reporting (NFRF), specifically Trade and Transaction Reporting (T&TR) remains a significant challenge for financial services firms. With over 400 reportable data points across the three main UK/EU regulations, MiFID II, EMIR and SFTR, requirements are complex and changes to the regulations continue to evolve. Even though reporting requirements have been in effect for over a decade, the regulator is becoming more sophisticated in their monitoring, meaning organisations require sound operating models and robust control frameworks to mitigate the risk of misreporting and potential regulatory scrutiny.

Five things you should know about the topic

1 Increased regulatory scrutiny

Firms continue to report incorrectly and in the past 7 years the FCA has fined large Tier 1 Sell Side firms up to £35m but also smaller firms have been penalised with the first MiFID II fines in 2025 for two brokers, in excess of £1m. The regulator continues to proactively identify inaccurate transaction reports, having strengthened their supervisory capabilities with a dedicated data quality team. The FCA's MarketWatch Newsletters (81, 82 & 84) focus on deficiencies in firms' operating models that result in breaches.

3 Changes to UK & EU Regulatory Reporting

Requirements are continuously changing, and the industry has recently (2024) experienced multiple changes in the form of re-writes. Further changes to both UK and EU MiFID are due in 2028, with significant changes earmarked for 2030. Firms should have structured change frameworks in place, covering horizon scanning, technology changes and new business requirements.

5 Governance and oversight

Meaningful Management Information is essential for effective management of risks. Teams should be appropriately resourced, with clear accountability and dedicated committees as points of escalation.

2 Control framework

Firms should implement control frameworks which mitigate end-to-end process risks. Poorly designed controls with limited field coverage, restrict firms' ability to detect errors.

4 Rules interpretation, logic design and data lineage

Transaction reporting is complex and heavily reliant on the quality and accuracy of data, as most information is sourced upstream, there is a dependency on Front Office booking and trade capture systems. A single data point can be subject to multiple different interpretations, logic and eligibility. Misinterpretation of regulatory requirements and a lack of business context in reporting logic have also led to misreporting.

“The regulator is becoming more sophisticated in their monitoring, meaning organisations require sound operating models and robust control frameworks to mitigate the risk of misreporting”

Five things Internal Audit should do

1 Design a T&TR specific IA review

Given the complexities of transaction reporting, Internal Audit function should perform an end-to-end T&TR specific audit to assess whether the firm's reporting operating model is designed and operating in line with the applicable regulatory requirements and supports the completeness, accuracy and timeliness of reported data.

2 Control framework

Ensure that the controls review extends to the design and effectiveness of controls including preventive and detective controls (reconciliations), data flows from legacy systems and manual data inputs, as well as output from external reporting providers. Internal Audit should also consider the second line oversight such as Compliance Risk Assessments (CRAs) and monitoring and testing.

3 Change and breach management process

Internal Audit should verify the robustness of the change and issues management process, to ensure the effective governance and oversight of the issue lifecycle from identification to resolution. This should include coverage of errors, back reporting and omissions notifications to the regulator.

4 Rules interpretation and data mapping

Internal Audit should assess the governance and maintenance of regulatory interpretation, reporting requirements and data mapping documentation to ensure reporting logic remains aligned to applicable regulatory requirements and business processes.

5 Governance and oversight

Internal audit should check the effectiveness of the governance framework to include the relevant forums and committees, and the effectiveness of the Management Information. It would be prudent to assess ownership and accountability across teams, ensuring roles and responsibilities are understood, and the RACI is up to date.

31 Direct to Fund: a new dealing model for authorised funds

Overview

The Financial Conduct Authority (FCA) has finalised rules in Policy Statement PS26/7 to progress fund tokenisation and introduce a new direct to fund (D2F) dealing model for authorised funds effective from 30 April 2026. D2F is an optional alternative to the traditional Authorised Fund Manager (AFM) box model, allowing unit deals to be effected through a single-stage process directly with the fund, and changing the cash flows of subscriptions and redemptions which may reduce reliance on AFM client money arrangements. The model aims to simplify fund operations, enable consistency across jurisdictions, and enhance competitiveness of UK funds whilst helping firms adapt to future market changes.

Five things you should know about the topic

1 A model for the future

The model is available to both conventional and tokenised authorised funds and allows different dealing models within a fund or sub-fund. It is intended to support efficiency, atomic settlement and alignment with wider market changes including tokenisation and T+1 settlement.

3 Navigating umbrella structures

Umbrella-level omnibus IAC accounts remain challenging under protected cell legislation, and the FCA continues to work with the Treasury to clarify its application. Most firms are likely to need individual sub-fund IAC accounts unless legal advice supports an omnibus model that remains compliant, for example where all cash movements can be sequenced to prevent protected cell legislation breaches.

5 Governance and disclosure implications

Introducing D2F is expected to be treated as a notifiable change, with prospectuses updated to provide clear investor disclosures. Broader scheme documents must also be clear who is responsible for AML checks on underlying investors and who will carry out this activity.

2 Cash flow considerations

A D2F scheme must operate an issue and cancellation (IAC) account. Cash in the IAC account is scheme property, bringing fund pricing, spread of risk, reconciliation and depositary oversight considerations into scope.

4 Strengthened operational controls:

The final rules strengthen controls over daily or dealing-frequency reconciliations, prompt attribution of money, and treatment of unattributed scheme money, including escalation and return processes where money remains unattributed after 5 business days.

“The model aims to simplify fund operations, enable consistency across jurisdictions, and enhance competitiveness of UK funds”

Five things Internal Audit should do

1

Assess strategic readiness

Review governance over D2F adoption, including the business case, product scope, implementation plan, dependency mapping and alignment with tokenisation and T+1 programmes. Consider whether the change has clear risk acceptance criteria and senior management ownership.

2

Test IAC controls

Assess design and operation of IAC account processes and controls, including cash attribution, daily or dealing-frequency reconciliations and unattributed scheme money. Test the completeness and timeliness of exception reporting and remediation.

3

Challenge legal and scheme documentation

Evaluate whether protected cell legislation, scheme documentation, prospectus disclosures, AML responsibilities and investor communications have been assessed and clearly evidenced. Where omnibus IAC accounts are proposed, assess the legal advice obtained.

4

Review data and technology resilience

Assess whether systems, transfer agency data, bank account structures and reporting can support D2F, operational resilience and exception management. This should include interfaces with administrators, depositaries, banks and platforms.

5

Build ongoing assurance

Develop a multi-year plan covering implementation assurance, targeted post-go-live effectiveness, external assurance findings and lessons learned from early adoption. This should be revisited to ensure coverage as market practice and tokenisation models mature.

Changing SIPP regulation

Overview

In June 2026 the Financial Conduct Authority (FCA) released Consultation Paper CP26/20 with proposed new rules within the Conduct of Business Sourcebook (COBS) for firms operating self-invested personal pensions (SIPPs). The proposals target two areas where historic failures have crystallised customer harm:

- due diligence over investments and third parties; and
- the handling of pension scheme money and assets.

The proposed rules represent a step-change for SIPP operators, moving existing principles and guidance into more explicit Handbook requirements. The policy statement and final Handbook text is expected to be published H1 2027.

Five things you should know about the topic

1 Why the FCA is proposing new rules

Following several firm failures resulting in significant uncompensated consumer loss, the FCA aims to create a clearer control perimeter for SIPPs, providing a framework that drives consistent standards, strengthens trust, reduces the risk of scams and fraud, and achieves better consumer outcomes.

3 A new Pension Scheme Money and Assets (PSM&A) regime

The proposed COBS 19B PSM&A regime introduces CASS-style expectations for SIPP operators where the trustee is an unauthorised trustee not already subject to CASS. It includes requirements for member-level books and records, reconciliations and discrepancy resolution, and adequate organisational arrangements encompassing governance and oversight, training, and a documented risk management framework.

5 Implementation is likely to be material

The proposed rules are likely to require significant systems, controls and process changes, particularly where firms rely on data from third parties. This is reflected in the implementation periods of 12 months for due diligence, and two years for the PSM&A rules, with a further year possible where third-party data dependencies are identified.

2 Raising the bar on due diligence

The proposed COBS 19A due diligence rules will apply where consumers retain ongoing choice over investments. Firms will be required to perform initial and ongoing due diligence over relevant third parties and SIPP investments, with enhanced due diligence for higher-risk third parties and assets and perform ongoing monitoring to identify weaknesses in due diligence processes, policies or controls.

4 Increased accountability and regulatory oversight

The PSM&A regime will introduce senior management responsibility with individual accountability, as well as the requirement for an annual reasonable assurance external audit, and proposed monthly reporting to the FCA.

“The FCA aims to create a clearer control perimeter for SIPPs, providing a framework that drives consistent standards, strengthens trust, reduces the risk of scams and fraud”

Five things Internal Audit should do

1

Assess skill and capability

Assess the knowledge and skills those implementing the new regime and those required to provide effective assurance and oversight of the due diligence and PSM&A requirements. Identify capability gaps and consider leveraging specialist regulatory expertise to deliver targeted training and provide insight into evolving regulatory expectations.

2

Develop a roadmap to readiness

Assess governance over CP26/20 interpretation, impact assessment, implementation planning, milestones and dependencies, and reporting to senior management and the Board. This should include key areas such as risk management frameworks and policies and procedures, and alignment with other areas such as the Consumer Duty.

3

Design an ongoing programme of assurance

Build a multi-year assurance plan covering design, delivery and post-implementation effectiveness of controls for both COBS 19A and COBS 19B, including reliance on first and second line testing and any external assurance findings.

4

Assess internal audit coverage of COBS 19A

Under the proposed rules, the COBS 19A due diligence requirements will be out of scope of the annual external COBS 19B PSM&A audit. The COBS 19A rules also have the shortest implementation period. Internal audit should consider coverage of COBS 19A and assess how the new requirements might be incorporated into thematic reviews.

5

Focus on data integrity

With increasing reliance on data, including from third parties, internal audit should focus on the integrity and accuracy of pension scheme data from both its own systems and third-party systems that will be utilised in the new rulesets, particularly in key areas such as reconciliations.

Contacts



Aaron Oxborough
Partner

aoxborough@deloitte.co.uk



Matt Cheetham
Partner

mcheetham@deloitte.co.uk



Russell Davis
Partner

rdavis@deloitte.co.uk



Yannis Petras
Partner

ypetras@deloitte.co.uk



Marc McNulty
Partner

marmcnulty@deloitte.co.uk



William Macdonald
Associate Director

willmacdonald@deloitte.co.uk



Rubal Mehta
Associate Director

rubalmehta@deloitte.co.uk



Vince Greenaway
Senior Manager

vgreenaway@deloitte.co.uk



Jamie Whitehouse
Senior Manager

jlwhitehouse@deloitte.co.uk



Saroj Mandhwani
Senior Manager

smandhwani@deloitte.co.uk



This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP's affiliate (Deloitte Management Services Limited) is a shareholder in Deloitte EMEA BV (Deloitte EMEA). Deloitte EMEA is a member firm of Deloitte Touche Tohmatsu Limited (DTTL). DTTL and Deloitte EMEA do not provide services to clients. Services may be provided by other Deloitte entities within the global network of member firms, each of which are separate and independent legal entities. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2026 Deloitte LLP. All rights reserved.