The Risk Agenda 2027



Banking and Capital Markets (B&CM)

PwC

September 2026

Disruption is no longer an event to manage, it is the landscape to navigate



Nicole McManus

Partner,
Financial Services
Internal Audit Leader,
PwC UK

+44 (0) 7989 950485

nicole.r.mcmanus@pwc.com

As the Banking sector enters 2027, it does so dealing with a fast-changing world and amid a period of significant change. Geopolitical fragmentation, rapid technological development and evolving market structures are reshaping where firms compete and how financial services are delivered. At the same time, major regulatory reforms are moving into implementation, while cyber threats, third-party dependencies and interconnected markets continue to test resilience.

Disruption also creates a significant growth opportunity. Artificial Intelligence is changing how firms operate and make decisions, tokenisation has the potential to rewire market infrastructure, private capital is reshaping the financing ecosystem. regulatory reform is placing greater emphasis on proportionality, competitiveness and responsible innovation. The challenge for firms is to capture these opportunities without allowing speed, complexity or interconnectedness to undermine resilience and trust.

This matters beyond individual firms. The UK's financial and related professional services industry remains a strategic national asset, supporting investment, jobs and economic resilience. As highlighted in PwC's 2026 publication with TheCityUK, *No time to lose: Reasserting UK leadership in financial and related professional services*, the UK cannot take its position for granted. Global competition is intensifying and technology is rapidly changing the foundations of financial markets. The report argues that the opportunity is substantial if the UK can combine innovation with greater pace, proportionate regulation and effective mobilisation of capital, PwC modelling estimates an upside of up to £53bn of additional annual economic output by 2035.

For firms, growth and resilience therefore need to be considered together. Moving faster on AI, digital assets and market transformation requires confidence that governance and controls can keep pace. Greater use of external technology creates new concentrations and dependencies. More interconnected capital markets require firms to understand exposures across traditional organisational and product boundaries. And greater regulatory flexibility can place more, not less, emphasis on management judgement and evidence that risks remain appropriately controlled.

For Internal Audit, this creates an opportunity to support responsible growth while maintaining independent challenge. Assurance should increasingly focus on whether strategic change is delivering its intended outcomes, whether new risks and dependencies are understood, and whether controls operate effectively as firms move from implementation to scale. This means looking across traditional audit boundaries and providing timely assurance as business models, technology and markets evolve.

This year, our document covers the following areas:

- **Macro risk landscape:** The geopolitical and economic forces shaping financial markets and strategic decision-making.
- **Market shifts**: Structural shifts including technology and AI, tokenisation, workforce change and the growth of private credit.
- **Risk and regulatory hot spots**: Key areas including prudential reform, operational resilience and third-party reporting, T+1 settlement, cyber and frontier AI.

We hope this year's Agenda helps you consider not only where disruption is creating risk, but where responding to it differently can strengthen competitiveness and enable sustainable growth. The organisations best placed for 2027 will be those that can move with pace while retaining confidence in the resilience, governance and controls that underpin that change.

If you would like to discuss any aspect further, please do not hesitate to contact me or one of my colleagues whose contact details are at the end of this paper.

PricewaterhouseCoopers LLP, 7 More London Riverside, London, SE1 2RT T: +44 (0) 20 7583 5000, F: +44 (0) 20 7212 7500, www.pwc.co.uk

PricewaterhouseCoopers LLP is a limited liability partnership registered in England with registered number OC303525. The registered office of PricewaterhouseCoopers LLP is 1 Embankment Place, London WC2N 6RH. PricewaterhouseCoopers LLP is authorised and regulated by the Financial Conduct Authority for designated investment business and by the Solicitors Regulation Authority for regulated legal activities.

Contents

1 Section 1: Macro risk landscape

Geopolitical risk outlook	05
UK economic outlook	08

2 Section 2: Market shifts

When technology becomes the operating model	10
Artificial Intelligence and assurance: Governing, controlling and overseeing AI across the enterprise	14
Tokenisation: rewiring financial markets for growth	19
People, culture and workforce: Adapting to the future of work	21
Private credit: An interconnected web of capital, financing and risk	23

3 Section 3: Risk and regulatory hot spots

Regulatory landscape	28
The minimum viable company: protecting organisational viability through disruption	31
Managing external dependency and third-party risk in 2027	36
The changing shape of cyber risk – what leaders need to act now on	41
Frontier AI: Keeping pace with accelerating threats	46
PS26/2: Operational incident and third-party reporting	50
Implementation of Basel 3.1, Small Domestic Deposit Takers (SDDT) and operational resilience requirements	54
T+1 accelerated settlement	58
Wider Risk landscape	61

4 Section 4: Contact and glossary

Contact us	63
Glossary	64

Macro risk landscape



Geopolitical risk outlook

Geopolitical volatility is now a persistent feature of the global operating environment. The systems and structures that have helped govern the global system in recent decades are weakening and changing. Global powers, responding to this changing environment, are competing for influence, and looking to new diplomatic, economic and security relationships to do this. This is contributing to more frequent geopolitical shifts and shocks.



The politicisation of interdependence

Governments and other actors are showing a greater willingness to use economic dependencies as sources of leverage. Geopolitical risks are transmitted through systems on which organisations depend: **trade routes, supply chains, technology ecosystems, financial payments systems and access to strategic resources**. Trade and security are now critically interlinked, driving greater moves towards autonomy, self-reliance and protectionism. Diversified, resilient and secure supply chains and energy are increasingly balanced against efficiency or low-cost options.

Building adaptability and resilience

While organisations can prepare for some specific geopolitical scenarios, they cannot anticipate every eventuality. Instead, they should build the capacity to absorb shocks, maintain continuity, recover quickly and adjust strategies as political and economic conditions evolve. This requires three practical capabilities:

01

Build visibility: Map critical physical and digital dependencies beyond immediate suppliers, including routes, jurisdictions, infrastructure, technology providers and processing capacity. Identify contingency options including diversification, nearshoring or strategic stockpiling where appropriate.

02

Establish governance – Make it someone's problem: Set responsibilities and define how geopolitical developments are monitored, assessed, escalated and incorporated into commercial and resilience decisions. Move from passive horizon-scanning and build geopolitical considerations into decision-making.

03

Scenario planning: Use plausible disruption scenarios to examine whether the organisation can maintain critical services, identify alternatives and make decisions at sufficient speed.

Chokepoints: disruption as strategic leverage

The closure of the Strait of Hormuz has demonstrated how chokepoints and concentrated trade routes can be used as a source of strategic leverage, especially in conflicts with severe power imbalances. Disruption of these routes can have significant global repercussions, extending well beyond the conflict zone. And the risk extends beyond the direct loss of passage. Rerouting, insurance changes, port congestion and price volatility can transmit disruption across sectors and regions, including to organisations with no direct presence in the affected area.

With over 80% of traded goods by volume transported by sea, other actors may view chokepoint and trade route disruption as a viable tactic. Once a vulnerability has been demonstrated, the likelihood of chokepoint disruption becoming a recurring risk also increases. The repeated disruption of shipping through the Red Sea is an example of this. Houthi attacks that began in 2023 showed that the initial disruption was not a one-off event, but the emergence of a recurring risk. Although attacks periodically subsided, they later resumed, reinforcing the need to view such threats as enduring vulnerabilities rather than temporary crises.

These events are reinforcing the strategic importance of alternative routes and supply arrangements. In the Middle East, we are already seeing announced investments in new and expanded oil pipelines in the UAE, Iraq and Syria, aimed at reducing dependence on vulnerable maritime routes. Such investments illustrate a broader shift from supply chains designed primarily for cost and efficiency towards those that place greater value on security, diversification and resilience.

Visibility of concentrated routes and infrastructure is essential to building adaptable supply arrangements.

Geopolitical risk outlook (continued)

Trade fragmentation: from disruption to adjustment

Politically motivated and national security-related trade barriers are reshaping the global trade environment. Tariffs and other trade restrictions are increasingly being used not only to protect domestic economies, but to advance national security, industrial policy and geopolitical objectives. The result is not necessarily an end to global trade, but a more fragmented and compliance-intensive environment in which goods, technology, data and capital may face different restrictions across markets.

The initial disruption associated with rapid changes in US trade policy has given way to a period of adjustment, as countries and businesses adapt to a more protectionist environment. This is contributing to a greater reliance on regionalised trade networks and the reconfiguration of global supply chains. It also challenges just-in-time approaches to inventory that are vulnerable to shocks and rapid policy changes, reinforcing the growing need to balance resilience and efficiency.

For businesses, this can raise input costs, complicate market access and undermine supply-chain models designed primarily for efficiency. Divergent requirements across regions, including data-sharing restrictions, could increase costs or even make continued operation prohibitive. An increase in bilateral trade agreements, country-specific tariffs and rules of origin requirements could heighten the compliance burden on companies.

Organisations need to understand how changing trade relationships could reshape their markets, supply chains and operating models.

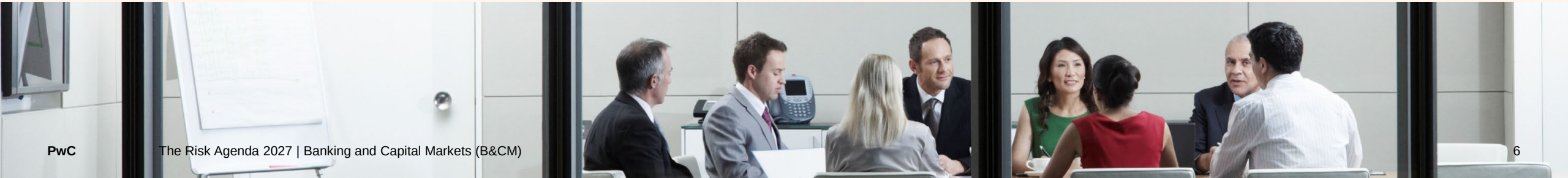
Critical minerals: new instruments of geopolitics

Access to critical minerals and rare earth elements is increasingly becoming linked to geopolitical competition. These materials are crucial for a wide range of products, but especially key to advances in tech, defence and energy transitions. As such, governments are now viewing them through the lens of national security and geopolitical leverage. As geopolitical risk rises and supply chains reconfigure, access to minerals and processing capacity will increasingly determine which companies can deliver growth, manage volatility and maintain investor confidence.

For UK and European companies, the risk is not only scarcity or price volatility, but exposure to political decisions made elsewhere. Trade disputes between the US and China in recent years have shown the impact of export controls, sanctions, trade retaliation, and stockpiling of these materials. Moreover, the geographic concentration of refining and processing exacerbates the risks, which may appear through supply-chain dependencies that companies do not directly control.

In an attempt to secure and diversify critical mineral supply, governments are taking a more active role in supporting new mines and refining and processing facilities to reduce the extent of this concentration in China. Many of the issues that previously discouraged this kind of investment remain though, such as high operating costs and tighter environmental regulation. National security and resilience are driving governments to subsidise and incentivise such developments to protect supply chains for tech, defence and critical manufacturing. Diversification can therefore add security and resilience but not necessarily reduce cost.

Dependencies in mining, refining and processing need to be visible within procurement, investment and continuity decisions.



Geopolitical risk outlook (continued)

Technology competition: control over critical ecosystems

The role of technology in geopolitical competition is continuing to increase, and control over AI technology and related infrastructure has become a strategic priority for major powers. Technology is now widely seen as a national security issue, and this lens can take precedence over commercial objectives.

The US and China are driving the use of trade barriers to limit competitors' technological progress. Restrictions span four main areas:

- **raw materials, including rare earth elements and critical minerals,**
- **components and manufacturing capability, including those needed for advanced technology such as chips,**
- **knowledge and intellectual property, including advanced processes, and**
- **data, compute and cloud infrastructure, including data sets and access to frontier AI models.**

The impacts of such competition and protectionism reach far beyond the tech industry. Businesses need to critically assess which geopolitical technology ecosystem they operate in, what control over data, models and systems they retain and what dependencies and concentration risks they face.

Businesses should monitor policy developments affecting AI export controls, cloud sovereignty, chip availability and open-source releases. They should also map where AI models are used, which provider and jurisdiction controls them, and whether each model is cloud-based, hosted in a regional data centre or hosted in a client-owned data centre.

Organisations need to understand which providers and jurisdictions control their critical models, data, infrastructure and components.



UK economic outlook



Resilience has bought time – but growth remains subdued

The UK economy has proved more resilient than many expected after several years of successive shocks. Real GDP grew by 0.6% in Q1 2026 and 0.4% in Q2. The IMF now expects the economy to grow by 1.0% in 2026 and 1.3% in 2027, having revised its 2026 forecast upwards by 0.2 percentage points, the UK was the only G7 economy to receive an upgrade in the latest round of forecasts.

Household and corporate balance sheets also provide some protection against further disruption, with UK corporate debt around its lowest level this century.

However, resilience should not be mistaken for a return to strong underlying growth. Inflation remains above target and vulnerable to external shocks, while much of the expansion in recent years has been concentrated in public-sector-dominated activities.

The bigger issue for 2027 is whether the UK can convert short-term resilience into stronger private-sector investment, productivity and real income growth.

Management teams should plan for a relatively low-growth environment in which demand, financing conditions and input costs may remain volatile. Business plans that depend on a rapid return to historically stronger growth or inflation falling smoothly back to target may warrant greater challenge and scenario testing.

Converting resilience into confidence and investment is the next step

Healthy balance sheets have not translated into a decisive increase in investment. Real UK business investment remains below its pre-2016 trend, while households continue to save more than before the pandemic. Higher labour costs, taxation, geopolitical uncertainty and uncertainty over future demand are all making firms more cautious about committing capital.

This sits within a wider global picture of weaker business confidence. PwC's 2026 Global CEO Survey found that only 30% of CEOs were very or extremely confident about revenue growth over the following 12 months, while almost a third said geopolitical uncertainty was making them less likely to undertake large new investments. The survey is global rather than UK-specific, but the underlying dynamic is relevant to an economy competing internationally for mobile capital. Encouragingly, the UK remains one of the leading destinations for planned international investment, selected by 13% of CEOs making cross-border investments – but competition from the US, India, the Middle East and other centres is intensifying.

There is also a risk that uncertainty reinforces short-termism. UK CEOs responding to the survey reported spending around 55% of their time on issues with horizons of less than one year and only 11% on issues extending beyond five years. For organisations facing AI disruption, changing trade patterns and major infrastructure and energy transitions, an overly short-term focus may itself become a strategic risk.

The challenge is to distinguish sensible caution from strategic inertia. Boards should scrutinise whether uncertainty is delaying investments that are important to long-term competitiveness, particularly in technology, skills, resilience and new sources of growth.

The UK's next growth model will depend on productivity, capital and competitiveness

The UK enters the second half of the decade with substantial investment requirements. Infrastructure, housing, defence, energy security, digitalisation and the transition to new technologies will all compete for capital at a time when the Government has limited fiscal headroom. Delivering these priorities will therefore depend increasingly on the UK's ability to attract and mobilise private investment.

There has been some recent evidence of UK productivity growth in 2026 and that, along with technology adoption, access to capital, predictable policy and regulation, skills and international competitiveness all determine whether investment remains in the UK or moves elsewhere. Capital and talent have become increasingly mobile, and the UK cannot assume that historic strengths will automatically translate into future investment.

AI is an important part of that productivity opportunity, but the benefits are not automatic. Our 29th CEO Survey shows that more than half of companies globally have yet to realise either higher revenues or lower costs from AI. The organisations achieving both are those embedding AI more broadly into their operating models and building the underlying technology, data, governance and workforce foundations needed to scale it.

For the UK, the central economic question is therefore shifting from resilience to renewal: whether policy, business investment and technological adoption can combine to lift productivity and create a stronger private-sector growth engine before fiscal, demographic and geopolitical pressures become more binding.

Strategy and risk assessment should increasingly consider the organisation's exposure to the UK's structural growth constraints as well as the economic cycle – including productivity, skills availability, infrastructure, energy costs, access to capital and the UK's relative attractiveness as a place to invest.

Market shifts



When technology becomes the operating model

Technology is no longer simply supporting the organisation. It increasingly determines how value is created, decisions are made, services are delivered and disruption is managed.

The defining issue for 2027 is not the emergence of any single technology. It is the combined effect of technologies becoming more intelligent, embedded, interconnected and resource-intensive, at a pace that is often too fast for governance, architecture, skills and assurance arrangements to keep up.

This creates a strategic tension. Technology offers one of the clearest routes to productivity, growth, innovation and improved services.

Yet, as organisations embed it more deeply into their operating models, they also create new dependencies and increase the consequences of failure. The challenge is no longer whether organisations are investing enough in technology. It is whether they can convert that investment into sustainable value without allowing complexity, concentration or speed to undermine control.

Four connected shifts are shaping this landscape.

01 Digital ambition collides with physical and capacity constraints

Digital services are often described as though they are intangible and infinitely scalable. In reality, cloud services, AI, digital platforms and data-intensive operations rely on physical infrastructure: advanced chips, data centres, telecommunications networks, electricity, cooling capacity and specialised engineering skills.

Demand for these resources is rising quickly. The International Energy Agency has reported that global data-centre electricity demand grew by 17% in 2025, while consumption from AI-focused data centres grew by 50%. Its updated outlook projects total data-centre electricity consumption to roughly double from 485 terawatt-hours in 2025 to 950 terawatt-hours in 2030, with bottlenecks emerging across power systems, advanced chip manufacturing and planning processes.

The strategic importance of the underlying infrastructure is becoming more explicit**.** The UK Government's 2026 data-centres factsheet describes data centres as critical to nearly all economic activity and public services and sets out plans to designate qualifying operators as essential services under the Cyber Security and Resilience Bill.

For corporate and public-sector organisations, these constraints can change the economics, timing and resilience of transformation. Capacity, location, energy availability, financing, supplier viability and access to specialist hardware and skills can determine whether a programme scales as planned, what it costs, where workloads can be hosted and how exposed critical services are to local or provider-level disruption. Technology plans therefore need to test their infrastructure and capacity assumptions as rigorously as their software functionality and business cases.



When technology becomes the operating model (continued)

02 Efficiency creates concentration risk and hidden dependency

Cloud platforms, software-as-a-service, shared infrastructure and specialist providers allow organisations to access capabilities that would be difficult or uneconomic to build independently. They support scalability, innovation and, in many cases, improved resilience.

However, the same standardisation that creates efficiency is concentrating important services around a relatively small number of providers and technology ecosystems. In July 2026, UK financial regulators began overseeing Amazon Web Services, Google Cloud, Microsoft and Oracle as the first Critical Third Parties to the UK financial sector, recognising that disruption or failure could affect multiple firms or markets at the same time. Although the regime is sector-specific, it illustrates the wider significance of common technology providers whose services underpin many organisations simultaneously.

Dependencies can also be difficult to see. An organisation may use multiple applications or suppliers while those services rely on the same cloud platform, identity service, software component, data provider or infrastructure location. Supplier diversity on paper may therefore conceal concentration risk deeper in the technology ecosystem.

The issue is not that organisations use external providers, those ecosystems are fundamental to modern technology. The issue is whether leaders understand where concentration exists, how easily critical services could be moved or substituted, and how failure could cascade across services, suppliers and customers.

03 Continuous change tests traditional control models

Organisations are making more technology changes, more frequently, across increasingly complex estates. Cloud platforms and software providers release changes continuously. Transformation programmes must integrate new technology with legacy applications. AI can both accelerate software development and increase the volume of code and configuration changes, while agentic AI is increasingly becoming a source of operational change in its own right. Meanwhile, organisations must continue operating the systems on which existing services depend.

The result is a difficult balance. Moving too slowly can leave an organisation uncompetitive, inefficient or dependent on obsolete technology. Moving quickly without sufficient control can introduce service disruption, security weaknesses and technical debt.

A June 2026 Basel Committee review – focused on banking, but relevant as a warning about complex technology estates – found that change-control gaps were the most frequently reported root cause of non-malicious technology incidents across the jurisdictions surveyed. Gaps in system design, development and testing were the second-most cited cause, while capacity issues and external dependency failures were also prominent. The review noted that the interplay between legacy systems, emerging technologies and rapid digitalisation compounds the complexity of change.

Control models built primarily around periodic approvals, project stage gates and retrospective reviews will find it increasingly difficult to match this pace. Governance and assurance models need to move further into architecture, development and deployment processes. This includes risk-based change controls, automated testing, secure-by-design principles, progressive deployment, dependency analysis and active monitoring of whether technology changes are delivering their intended business outcomes.

When technology becomes the operating model (continued)

04 Trust and resilience become prerequisites for scale

As technology moves into more decisions and critical services, technology failure increasingly drives business failure. Organisations must demonstrate not only that technology works in normal conditions, but that services and decisions remain secure, reliable, explainable and recoverable as adoption scales.

Trust should not be viewed as a communications issue that follows implementation. It is an outcome of design choices, operating discipline and organisational behaviour. PwC's 29th Global CEO Survey found that two-thirds of chief executives had experienced stakeholder trust concerns in at least one area of their operations during the preceding year, including AI safety, data privacy and transparency. Public companies experiencing the fewest trust concerns delivered total shareholder returns that were, on average, nine percentage points higher over the period examined than those experiencing the most concerns.

This changes the focus of resilience. Organisations must be able to detect when an automated decision process is degrading, contain an AI-enabled process operating outside expected boundaries, maintain critical services when a provider fails, and explain decisions made under pressure. Without these capabilities, organisations may be able to pilot new technology but struggle to scale it confidently. Trust and resilience are therefore not brakes on innovation, they are prerequisites for sustainable adoption.



These are not four independent trends. The wider use of AI increases demand for data, computing infrastructure and specialist providers. Greater reliance on common platforms can increase concentration and expand the potential impact of failure. Integrating new technologies into established estates increases the pace and complexity of change. As dependency grows, resilience and trust become more important to whether technology can be adopted at scale.

The underlying challenge is cumulative. Organisations are not managing more technology risks. They are operating in an environment where technology opportunity, operational dependency, organisational change and stakeholder trust are increasingly inseparable.

When technology becomes the operating model (continued)

Questions for leaders

Where has technology become part of a critical business service?

Leaders need visibility beyond major applications to the data, AI models, platforms, infrastructure, suppliers and skills supporting important outcomes.

Are technology investments simplifying the operating model or adding another layer of complexity?

Adoption levels are not evidence of value. Leaders should understand how investment is improving outcomes and whether legacy processes and systems are being removed, integrated or merely worked around.

Where are the hidden concentration points?

Organisations should look beneath direct suppliers to shared cloud platforms, identity services, common software components, data providers and infrastructure locations.

Are controls evolving at the same pace as delivery?

The organisation should be able to show how risk, security, resilience and accountability are embedded into architecture and change, rather than applied mainly after implementation.

How would the organisation continue operating if a critical technology or provider became unavailable, unreliable or untrusted?

Resilience planning should address credible degraded modes of operation, decision override and recovery – not only conventional disaster-recovery scenarios.

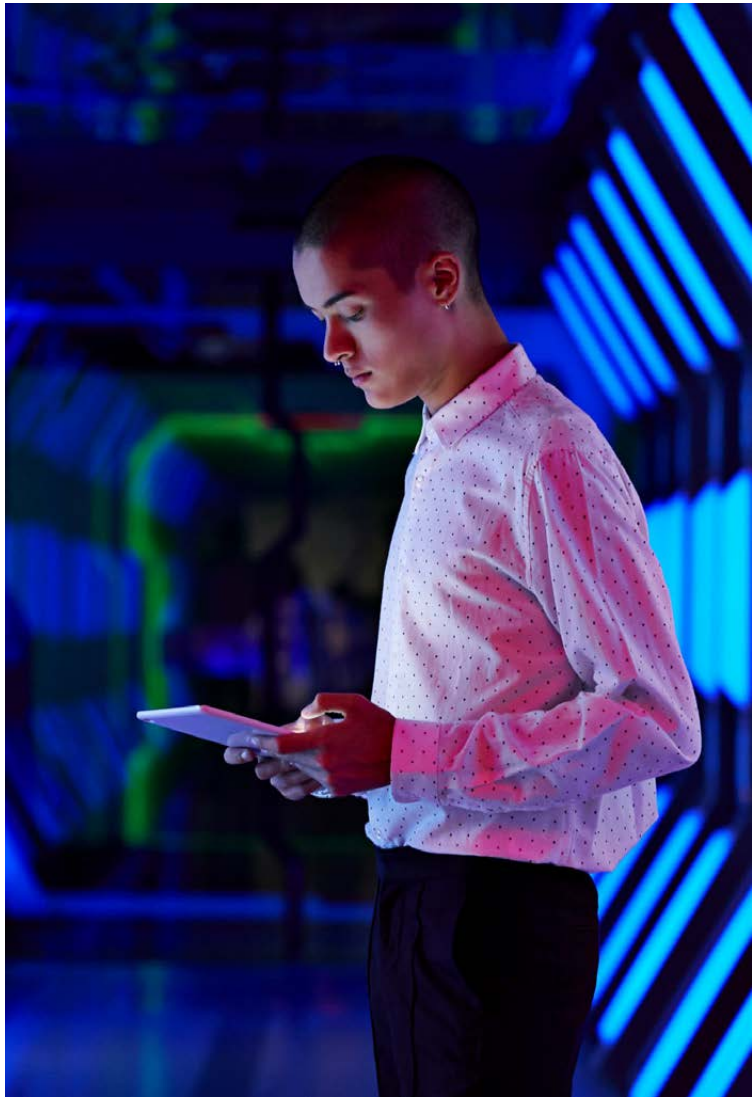
Internal Audit considerations

Internal Audit should avoid assessing individual technologies in isolation. Assurance should follow both the value chain and the dependency chain: from the intended business outcome through the process, data, technology, model, supplier and infrastructure supporting it.

This requires Internal Audit to move further upstream. In-flight assurance over transformation programmes, architecture decisions and control-by-design can provide more value than identifying weaknesses after deployment. Audit coverage will also need to become more dynamic, recognising that annual plans and periodic reviews may not reflect the speed at which technology dependencies change.

Assurance functions should consider whether they have sufficient capability to assess technology value, architecture, resilience, AI-enabled decision-making, supplier concentration and modern change practices. This does not mean building deep expertise in every emerging technology. It means having enough knowledge to identify where specialist input is required, challenge management's assumptions and connect technical issues to business outcomes.

The organisations that gain most from the next wave of technology will not necessarily be those that adopt every innovation fastest. They will be those that can make technology change repeatable, trusted and resilient – turning speed into value without allowing complexity to become fragility.



Artificial Intelligence and assurance: governing, controlling and overseeing AI across the enterprise



Boards and audit committees increasingly expect a clear answer to three questions: is AI being used within agreed boundaries, is it producing acceptable outcomes, and does accountability remain clear throughout its lifecycle? Assurance over AI is the coordinated evidence that governance, risk management and controls over the organisation's use of AI are appropriately designed, implemented and operating effectively. It should extend from the identification and classification of AI use cases through approval, development or procurement, deployment, monitoring, change, incident response and retirement.

Why this matters for 2027

AI is moving from experimentation towards enterprise deployment, although the value achieved remains uneven. PwC's 2026 Global CEO Survey found that only 12% of CEOs reported achieving both increased revenue and lower costs from AI, while 56% reported neither benefit. Organisations achieving stronger returns were further ahead in establishing foundations such as a defined roadmap, formalised responsible-AI and risk processes, suitable technology and an enabling culture. PwC's 2026 AI Jobs Barometer also reports substantially stronger productivity growth among companies most exposed to AI. The objective of governance should therefore not be to slow adoption, but to enable AI to scale in a controlled, accountable and value-led way.

At the same time, AI capability is advancing rapidly. Frontier AI refers to the most capable models available at a given point in time, but its implications are not confined to a small number of frontier-model developers. Capabilities can diffuse into smaller, cheaper and open-weight models and become embedded in widely used third-party products and services. Increasingly, models are also being incorporated into agentic systems that can plan, make decisions and take sequences of actions with limited human intervention. Governance must therefore address not only the use case originally approved, but also changes in capability, model or service version, tool and data access, autonomy and the system's role within the wider business process.

Governance is consequently both a risk issue and a value issue. PwC's UK AI performance research found gaps between UK respondents and global AI leaders in areas including the strength of their AI roadmaps, alignment between AI and business objectives, and senior accountability for outcomes. It also highlights that clear rules, proportionate checkpoints and effective senior oversight can give organisations greater confidence to scale successful use cases.

AI risk is better treated as cross-cutting than as a separate silo. Existing owners across model risk, data and privacy, technology and cyber, conduct, third-party risk and operational resilience should adapt their standards and monitoring for AI-specific risk drivers. A common intake process can route each use case to the relevant risk disciplines. Existing model risk management processes may provide a useful anchor, but should not become the sole lens given the significance of non-model risks such as data leakage, prompt injection, inappropriate or harmful outcomes, third-party and embedded AI, and increasing autonomy.

Regulatory expectations are also becoming operational. In the UK, the FCA published the Mills Review in July 2026. The EU AI Act's enforcement architecture is now active, and transparency requirements for certain AI systems began applying on 2 August 2026.

Following the AI Omnibus that entered into force on 27 July 2026, the main requirements for Annex III high-risk AI systems are scheduled to apply from 2 December 2027, with later application for AI embedded in regulated physical products. The high-risk regime includes lifecycle risk management, data governance, documentation, record-keeping, human oversight, monitoring and serious-incident reporting obligations. Organisations will need to understand whether they act as a provider, deployer or another participant in the AI value chain, as their obligations differ.

The control challenge extends beyond centrally developed models. AI may be embedded in third-party platforms, existing applications, employee tools and end-to-end business processes, making it difficult to identify where it is being used, which decisions or actions it influences and who remains accountable. Boards and audit committees therefore need reliable evidence that material AI risks are understood, ownership is clear and controls are embedded wherever AI is developed, procured or used. This includes mechanisms capable of identifying capability changes and control weaknesses, escalating issues and supporting timely intervention before they result in customer, regulatory, operational or reputational harm.

Artificial Intelligence and assurance: governing, controlling and overseeing AI across the enterprise (continued)



The key risks and opportunities

An incomplete view of the AI estate: An inventory that records only centrally approved or internally developed models may miss AI embedded in supplier products, business applications, employee tools and wider digital services. Without a complete inventory and a consistent method for assessing materiality, organisations may apply excessive governance to low-risk productivity tools while failing to identify AI that materially influences customers, employees, safety, operations, financial outcomes or regulatory compliance.

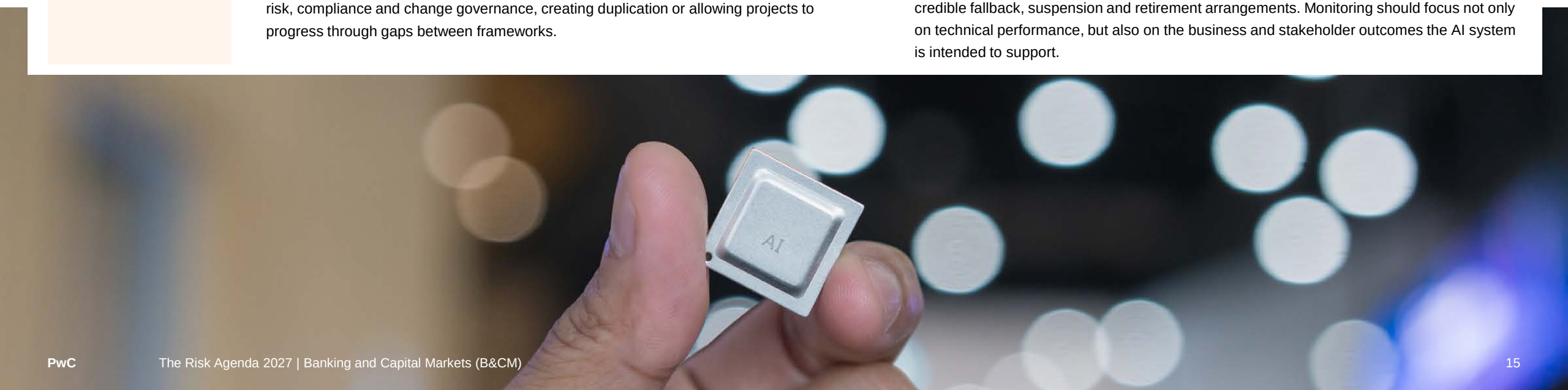
The opportunity is to establish a single, risk-tiered view of enterprise AI. Each material use case should be linked to its purpose, business owner, technical or model owner, data sources, third parties, level of autonomy, affected stakeholders, applicable requirements and lifecycle status. Governance and assurance can then be proportionate to the potential impact.

Governance that is not embedded in business decisions: AI policies and governance forums can coexist with unclear accountability for outcomes, human overrides, control failures and incidents. Approval processes may also sit outside existing product, technology, risk, compliance and change governance, creating duplication or allowing projects to progress through gaps between frameworks.

The opportunity is to integrate AI into the organisation's established governance and operating model. Clear decision rights should define who can approve a use case, accept residual risk, authorise material changes, suspend use and determine whether an incident requires escalation or notification. Proportionate checkpoints can then help good ideas move faster while directing stronger challenge towards higher-risk applications.

Static controls for systems that continue to change: A one-off risk assessment or pre-deployment validation does not demonstrate that an AI system will remain effective. Performance may change as data, prompts, model versions, supplier services, user behaviour or the surrounding business process changes. Manual review and spreadsheet-based monitoring may also become difficult to sustain as the number and complexity of AI use cases grow.

The opportunity is to design lifecycle controls that can operate at scale. These may include defined performance and risk thresholds, controlled changes, monitoring of data and outcomes, revalidation triggers, exception management, access controls, reliable logs and credible fallback, suspension and retirement arrangements. Monitoring should focus not only on technical performance, but also on the business and stakeholder outcomes the AI system is intended to support.



Artificial Intelligence and assurance: governing, controlling and overseeing AI across the enterprise (continued)



The key risks and opportunities

Human oversight that exists in name only: Describing an AI process as "human-in-the-loop" provides limited assurance if the individual reviewing the output does not understand its limitations, lacks time or authority to challenge it, or cannot evidence the judgement applied. Overreliance can result in AI recommendations becoming decisions in practice, even where formal accountability remains with a person.

The opportunity is to define meaningful human oversight. Staff should understand when challenge is required, what evidence is available, when an output must be overridden or escalated and how the final decision should be recorded.

In practice, reviewers need sufficient time, knowledge and authority to challenge or halt an AI-supported action, and the level of human involvement should reflect the impact and reversibility of the decision. High-impact or legally consequential decisions may require a person to remain in control, while routine, reversible activity can be monitored by exception using automated guardrails, thresholds and kill switches. This allows organisations to automate at scale without turning human review into a high-volume manual queue.

Assurance should test how people interact with AI in live processes, rather than relying only on role descriptions, training records or stated governance arrangements.



Incidents and third-party risks that fall between existing frameworks: AI-related events may present as a data breach, incorrect decision, discriminatory outcome, customer complaint, operational failure, cyber incident, intellectual-property issue or supplier problem. Where organisations rely solely on generic technology, operational-risk or whistleblowing channels, the AI element may not be identified quickly enough to support effective containment, investigation, reporting and learning.

Third-party systems add further complexity. Organisations may have limited visibility of supplier models, training data, controls, subcontractors, model changes or service concentration, while remaining accountable for the outcomes created through their own business processes.

The opportunity is to integrate AI into existing incident, crisis and third-party risk arrangements while introducing sufficient AI-specific criteria. This includes a common incident taxonomy, clear severity and reportability thresholds, preservation of relevant records, defined supplier notification requirements, investigation capability and a process for translating incidents and near misses into control improvements.

For third-party AI, assurance should be proportionate to impact: stronger independent evidence where supplier AI materially affects customers, decisions or sensitive data, and contractual attestations or inherited controls for lower-risk uses. Due diligence should cover data use, material service changes, sub-processors, incident notification, audit and exit rights. Ultimately, accountability for risk should not be outsourced, and so supplier evidence should be supplemented by the organisation's own validation where needed to ensure third-party AI meets the defined AI governance and operating standards.

Assurance activity without an integrated assurance view: AI risks often cut across technology, data, cyber security, privacy, legal, compliance, model governance, operational risk, third-party risk and business management. Several teams may therefore review parts of the same use case while important lifecycle stages or business outcomes receive limited attention.

The opportunity is a coordinated assurance strategy that identifies which material risks and controls are covered by management, the second line, Internal Audit and specialist providers. Reporting to the board should distinguish the existence of a framework from evidence that controls are embedded and operating effectively.

Artificial Intelligence and assurance: governing, controlling and overseeing AI across the enterprise (continued)



Questions for leaders

01

Where is AI being used?

Does the inventory cover internally developed systems, third-party and embedded AI, employee-accessed tools and AI introduced through wider transformation programmes?

02

Which AI uses matter most?

Are use cases classified consistently according to their potential impact on people, customers, employees, safety, operations, financial outcomes, legal obligations and reputation?

03

Who is accountable?

Is there a named business owner for the outcome, alongside clear technical, data, risk and compliance responsibilities? Who can accept risk, approve material change or suspend use?

04

What must be true before deployment?

Are expectations clear for data quality, testing, security, privacy, legal and regulatory assessment, explainability, human oversight, resilience and operational readiness?

05

What evidence shows that controls operate in practice?

Can management demonstrate that approvals, restrictions, monitoring, change controls and escalation arrangements are being followed, rather than relying on policy statements or self-certification?

06

How do we know that outcomes remain acceptable?

Are performance, errors, drift, bias, overrides, complaints, incidents and stakeholder outcomes monitored at a level that allows timely intervention?

07

Are incident and third-party arrangements fit for AI?

Can the organisation identify the AI contribution to an event, contain or suspend the relevant system, preserve evidence, meet notification obligations and obtain timely information and support from suppliers?

08

What assurance does the board receive?

Is there an integrated view of assurance coverage, control weaknesses, accepted risks, overdue remediation and the evidence supporting management's conclusions?

Artificial Intelligence and assurance: governing, controlling and overseeing AI across the enterprise (continued)

Internal Audit considerations

Internal Audit should treat assurance over AI as an enterprise governance, risk and operating-model question, not solely as a technology or model review. Its programme should combine an assessment of the organisation-wide framework with targeted reviews of material AI use cases.

Internal Audit should consider whether:

01

The AI inventory is sufficiently complete, current and supported by clear ownership, materiality assessment and regulatory mapping.

02

AI strategy, risk appetite, policies and governance arrangements are aligned with wider organisational objectives and established risk and control frameworks.

03

Lifecycle controls cover use-case intake, approval, data, development or procurement, validation, deployment, access, change, monitoring, incident management and retirement.

04

Material use cases can be traced end-to-end – from input data and model output through human review to the final decision and the resulting business or stakeholder outcome.

05

Human oversight is meaningful in practice, with users able to understand, challenge, override, escalate and document material decisions.

06

Third-party due diligence, contracts and monitoring address transparency, data use, performance, security, supplier changes, incident notification, resilience, concentration and exit.

07

Material AI use cases undergo appropriate testing and validation, including adversarial testing and red-teaming where proportionate to the risk, with identified weaknesses addressed before deployment.

08

Post-implementation monitoring and impact assessments are in place for material AI use cases to identify changes in performance, risk and outcomes, with issues escalated and remediated appropriately.

09

Board and committee reporting presents a balanced view of value, risk, control performance, incidents, limitations, accepted risk and remediation.



A critical distinction is needed between design, implementation and operating effectiveness. An approved AI policy, governance committee or inventory demonstrates design at most. Internal Audit should seek evidence from actual approvals, test results, monitoring records, changes, overrides, incidents, complaints, outcome analysis and completed remediation.

The organisations making real progress in this tend to start with a focused scope, a complete view of where AI is actually used, a small number of material use cases traced end-to-end, and honest reporting on what the evidence does and does not yet show – and extend coverage as the AI estate grows. Answering these questions well requires governance, data, technical, regulatory and audit expertise, combined with a practical risk and controls lens that keeps pace with AI's ever-evolving nature.

Tokenisation: rewiring financial markets for growth

Tokenisation represents assets and the rights attached to them on shared digital infrastructure. It can bring issuance, ownership records, transfer and settlement onto connected infrastructure, reducing reconciliation between separate systems and enabling more automated processing. Greater adoption could also affect the roles of intermediaries and the way financial products are issued, distributed and settled.



UK policy is now focused on live implementation and scale. Tokenised markets will need to connect effectively with settlement assets, payment infrastructure and existing market systems. Interoperability across platforms and jurisdictions will be important if firms are to avoid creating additional fragmentation. Common standards and connectivity are therefore becoming a practical requirement for broader market adoption.

Tokenisation can reduce transaction costs, improve capital and liquidity efficiency, and support new products and distribution models. Commercial outcomes will depend on where firms choose to participate and the role they play in emerging market structures. Early activity may give firms greater influence over standards, infrastructure and customer propositions as new markets and revenue models develop.

Activity is increasingly focused on established wholesale markets, including digital cash, government bonds, funds and equities. These use cases depend on effective settlement assets and payment infrastructure alongside tokenised securities.

The UK Government's Digital Markets Champion report reinforces this direction, with an initial focus on demonstrating an end-to-end tokenised repo transaction and addressing barriers to wider adoption.

PwC and Barclays estimate that UK annual economic output could be up to £22bn higher by 2035, rising to £33bn in an upside scenario. The Digital Markets Champion report cites this analysis in its case for UK action. The benefits reflect potential gains from productivity, investment, lower transaction costs and more efficient use of capital across financial services and the wider economy.

Scaling tokenised markets introduces risks across technology, operations, legal frameworks and market structure. Tokenised assets must work alongside settlement assets, payment infrastructure, existing systems and third-party providers. Firms will need to address settlement finality, custody, resilience, liquidity, financial crime and legal certainty, while also managing the cost and complexity of running legacy and tokenised infrastructure in parallel.

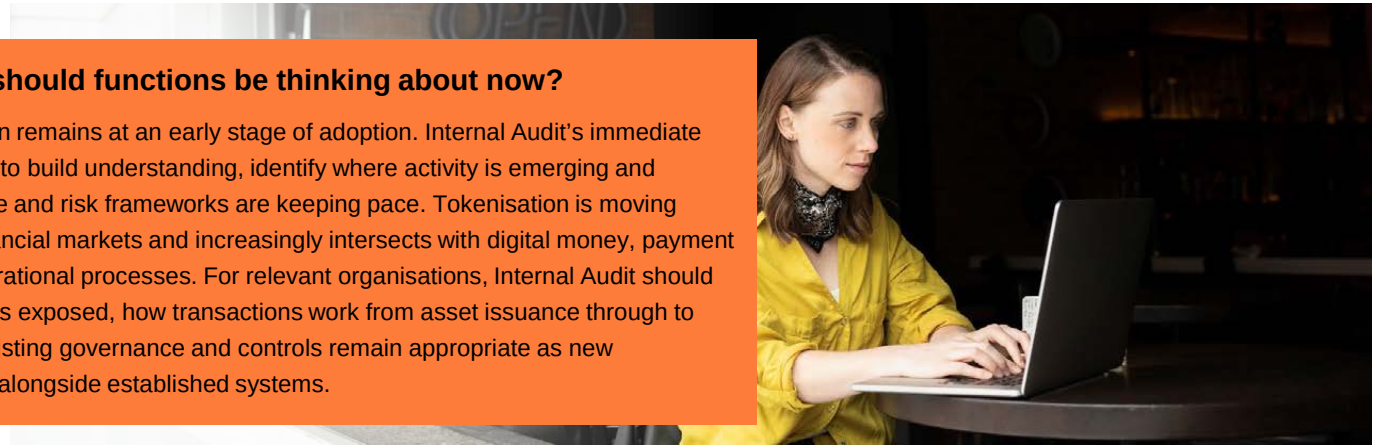
The UK regulatory framework is moving from experimentation towards live adoption.

In May 2026, the FCA and Bank of England set out a joint vision for tokenised wholesale markets, envisaging tokenised securities, cash and collateral operating across issuance, trading, clearing and settlement. They expect tokenised and traditional infrastructure to coexist, supported by interoperability and a technology-neutral regulatory approach focused on the underlying activity, rights and risks.

The prudential treatment of tokenised assets is also evolving. The PRA has indicated that tokenised traditional assets should generally receive comparable treatment to non-tokenised equivalents where the underlying legal rights and risks are the same, although the longer-term framework remains under development.

Alongside this, the FCA finalised its wider cryptoasset regulatory framework in June 2026, covering areas including prudential standards, conduct, safeguarding, market integrity, operational resilience and financial crime. The FCA and Bank of England are also developing their approach to systemic stablecoins and their potential role as settlement assets.

Tokenisation: rewiring financial markets for growth (continued)



Internal Audit: what should functions be thinking about now?

For many firms, tokenisation remains at an early stage of adoption. Internal Audit's immediate priority should therefore be to build understanding, identify where activity is emerging and assess whether governance and risk frameworks are keeping pace. Tokenisation is moving quickly into established financial markets and increasingly intersects with digital money, payment infrastructure and core operational processes. For relevant organisations, Internal Audit should understand where the firm is exposed, how transactions work from asset issuance through to settlement, and whether existing governance and controls remain appropriate as new infrastructure is introduced alongside established systems.

Internal Audit considerations:

Mapping exposure and materiality

Identify where tokenisation is entering the firm through products, pilots, partnerships, client activity and strategic programmes. The assessment should also cover indirect exposure through counterparties, custodians, settlement providers and market infrastructure. This provides a clearer view of where tokenisation could change existing risks or create new dependencies as activity grows.

Governance and accountability

Assess whether tokenisation activity has clear ownership, appropriate senior oversight and defined risk appetite. Legal, risk, compliance, technology, operations and treasury may all have important roles. Accountability needs to remain clear where activity crosses traditional organisational boundaries or relies on external infrastructure, technology providers and other market participants.

Settlement and digital money

Understand how tokenised assets are settled and what form of money or settlement asset is used. This may include commercial bank money, tokenised deposits, stablecoins, central bank digital money or existing central bank money accessed through upgraded payment infrastructure. Internal Audit should consider settlement finality, liquidity, funding, intraday risk and how the asset and settlement legs remain synchronised.

Asset lifecycle, custody and controls

Follow the asset from issuance through transfer, servicing and redemption. Understand when legal ownership changes, how transactions are authorised and how assets and associated rights are controlled. Relevant areas include custody, wallets and key management, smart contract governance, permissions, corporate actions and reconciliation between tokenised records and other books and records.

Interoperability, resilience and third parties

Assess how tokenised infrastructure connects with payment systems, settlement assets, existing technology and other market participants. New dependencies may arise across networks, custodians, technology providers and market infrastructure. Internal Audit should consider resilience, concentration risk, data flows, access arrangements and the controls required when transactions cross different platforms or operating environments.

Managing the move to scale

Consider whether governance and controls established for pilots remain appropriate when activity enters production and transaction volumes increase. Firms may operate tokenised and legacy infrastructure in parallel for an extended period, creating additional reconciliations, processes and dependencies. Internal Audit should reflect these changes in existing technology, markets, treasury, operations and transformation coverage as exposure becomes material.

Internal Audit needs to understand how tokenisation changes existing risks, controls and dependencies, and reflect those changes in its coverage as adoption grows.

People, culture and workforce: adapting to the future of work

Workplaces are moving towards a future in which technology skills become more widely embedded while distinctly human capabilities such as judgement, creativity and empathy remain increasingly important.

Technology, shifting skills needs, economic pressures and changing employee expectations are reshaping how organisations think about their workforce. AI is accelerating this transition, but the implications go well beyond the adoption of new tools. Organisations increasingly need to reconsider how work is organised, which capabilities they need, how careers develop and where people add greatest value alongside technology.

AI has the potential to improve productivity and augment human capability, while changing the skills required within existing roles and creating new ones. Organisations should seek to understand how roles and tasks will evolve, where skills gaps will emerge and how the workforce can adapt at sufficient pace.

Organisations need to bring their people and technology strategies together, giving employees the skills, confidence and opportunities to participate in change rather than treating workforce impacts as a downstream consequence of transformation. PwC's latest UK Workforce Hopes and Fears survey highlighted the importance of connecting learning, career frameworks, reward and the employee proposition around a clearer view of how work is changing.

As technology changes the tasks people perform, organisations will need to think differently about capability. The primary activity is no longer recruiting people into defined roles and periodically refreshing their skills. Jobs themselves are becoming more fluid, with technology taking on some activities, augmenting others and increasing the importance of capabilities such as judgement, creativity, leadership and interpersonal skills.

The changing nature of work also raises questions about how people build experience. AI and automation can remove routine activity, but that activity has historically provided an important training ground through which employees developed technical knowledge, judgement and confidence.



Ensuring that the workforce continues to develop the experience needed for tomorrow's specialist, leadership and decision-making roles should be front of mind for leaders.

Employees will also judge transformation through what it means for their own careers. Skills development, job security and credible opportunities to progress are increasingly intertwined. Organisations that ask people to continually adapt without providing a clear path forward risk weakening engagement and trust.

Successful workforce transformation will depend as much on culture, leadership and employee engagement as on technology

The changing workforce creates opportunities, but there is a risk that those opportunities are not experienced equally. Existing differences in participation, pay, progression and access to development remain persistent, while technological change introduces another dimension: who has access to new skills, emerging roles and the career opportunities created by transformation?

Expectations around workforce transparency are also becoming more demanding. Gender pay gap reporting is moving from disclosure towards action and accountability, while organisations may face a broader and increasingly interconnected set of workforce reporting requirements.

People, culture and workforce: adapting to the future of work (continued)

Questions for leaders

- How will our workforce need to change as our strategy and technology evolve? Do we understand which activities, roles and capabilities are likely to become more, or less, important?
- Are we building the skills we will need quickly enough? Is learning embedded into workforce planning and career development, or predominantly reactive to immediate capability gaps?
- How will people build careers in a more technology-enabled organisation? If traditional entry-level or developmental work changes, how will employees acquire the experience and judgement required for future specialist and leadership roles?
- Will different parts of our workforce benefit equally from change? Are there meaningful differences in access to technology, development, progression or emerging opportunities that could widen existing workforce inequalities?
- Do our people understand and trust the direction of travel? Are leaders communicating clearly about how work is changing and giving employees credible reasons to engage with, rather than resist, transformation?
- Can we demonstrate that our people interventions are working? Do workforce data and employee insight enable us to identify root causes, measure outcomes and change course where actions are ineffective?

Internal Audit considerations

Internal Audit should look beyond whether people policies, training programmes and reporting processes exist, and assess whether the organisation's workforce arrangements are enabling strategy while managing the risks created by significant change.

Workforce strategy and governance: Assess whether management has translated strategic and technology change into a credible view of future workforce needs, with clear ownership, assumptions and plans for roles, skills and capacity.

Skills and capability: Test how management identifies capability gaps and whether recruitment, reskilling and development activity is addressing them in practice. Consider outcomes and workforce coverage, rather than relying primarily on training completion metrics.

Career and workforce redesign: Assess whether changes to roles and processes have considered the longer-term implications for career pathways, development of experience, succession and critical capability.

Culture and employee experience: Use employee insight alongside management information to assess whether the organisation's stated culture and transformation narrative are reflected in how change is experienced across the workforce.

Fairness and workforce outcomes: Assess whether management understands differences in recruitment, progression, reward, retention and representation, whether interventions address underlying causes, and whether their effectiveness is being measured.

Workforce data and reporting: Review the quality, consistency and governance of data used for workforce decisions and external reporting, including whether reporting is connected to meaningful management action rather than operating primarily as a compliance exercise.



Private credit: An interconnected web of capital, financing and risk

Private credit broadly refers to loans or credit investments originated outside public debt markets and typically provided by private funds, asset managers or other institutional capital rather than being broadly syndicated or traded

Transactions are usually privately negotiated, comparatively illiquid and tailored to the borrower, with bespoke structures, covenants and collateral packages. Direct lending has historically been associated with sponsor-backed middle-market companies, but the market now spans a much wider range of financing needs – including asset-based finance, real estate and infrastructure debt, equipment finance, receivables, consumer and specialty finance.

The interconnectedness increases links between private credit, insurers and private equity firms which might highlight an increase in opacity, concentration risk and regulatory arbitrage.

This expansion matters because private credit increasingly sits between traditional bank lending and public debt markets. Borrowers can access capital directly from institutional investors, while banks remain involved through origination, warehousing, co-lending, subscription lines, NAV financing, back leverage, servicing and risk-transfer structures. In practice, the development of private credit is therefore less a simple transfer of lending from banks to funds and more a rewiring of the credit ecosystem.

Growth as an asset class

Private credit's growth has been substantial. Global private credit assets under management now stand at **more than $2 trillion and are expected to reach $3.4 trillion by 2030*.** The US is the most mature market, accounting for roughly 70% of global private credit, while the UK and Europe are among the fastest-growing regions.

The asset class is also broadening in both scale and scope. Private lenders are increasingly targeting larger companies and moving beyond the mezzanine and private-equity-oriented lending that characterised the market historically, to support global investment needs across Artificial Intelligence, Digital Assets and Infrastructure.

This change in scale is important for leaders because private credit is no longer relevant only to alternative asset managers. Banks, insurers, pension funds, corporates and wealth channels are all interconnected – as borrowers, investors, financiers, counterparties or distributors. The more the market expands across the capital stack and into new asset types, the more difficult it becomes to understand exposures by looking at any single product or legal entity in isolation.

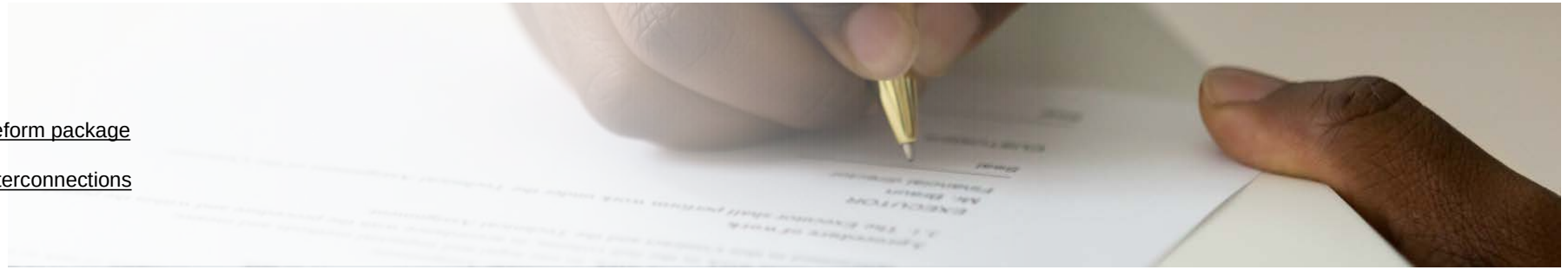
Further reading

PwC Global Private Credit Survey 2026

PwC At a Glance – HMT and FCA set out new UK AIFM reform package

PwC At a Glance – FSB turns spotlight on private credit interconnections

Bank of England Private Markets SWES Scenario



Private credit: An interconnected web of capital, financing and risk (continued)

Several structural forces have contributed to growth

01 A pull-back in some areas of bank lending

Post-financial-crisis regulation, tighter capital and liquidity requirements and changes in bank risk appetite have reduced balance-sheet capacity for some forms of mid-market, leveraged and bespoke lending. Private capital has been able to fill part of that gap, while banks increasingly participate through distribution, partnerships and financing rather than holding the full funded exposure.

02 Borrower demand for speed, certainty and flexibility

Private credit can provide tailored structures, bilateral or club-style negotiation, tailored covenants, delayed-draw components, bespoke collateral and greater certainty of execution. For borrowers undertaking acquisitions, refinancing or growth investment, those features may be more valuable than achieving the lowest headline cost of debt.

03 Investor demand for income and diversification

Private credit has attracted institutional investors seeking illiquidity premia, floating-rate income and senior-secured exposures outside public markets. Insurance companies and pension funds have been important sources of capital, and there is growing access for private wealth and retail through semi-liquid structures.

04 The growth of private markets and the need for financing solutions around it

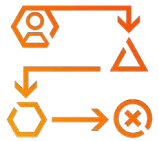
Sponsor-backed companies have remained a core source of demand, while slower exits and refinancing needs can increase demand for private capital across acquisition financing, refinancings, follow-ons and liquidity solutions. The interaction between private equity sponsors, private credit managers and banks has therefore become an increasingly important part of the market.

05 Expansion into asset-based and specialty finance

Growth is no longer limited to corporate cash-flow lending. Private capital is increasingly financing pools of assets and contractual cash flows, including receivables, equipment, infrastructure and other specialist assets. This materially increases the addressable market and creates different risk drivers from traditional direct lending.



Private credit: An interconnected web of capital, financing and risk (continued)



What regulators are focusing on

Regulatory attention is increasingly centred on whether the system can identify and absorb stress as private markets become larger and more connected.

- **Interconnectedness with banks and institutional investors** – In its 2024 thematic review, the PRA found that management of PE-linked exposures was largely siloed across business lines and business units, with a number of banks unable to identify and systematically measure combined credit and counterparty exposures within its risk monitoring data.
- **Visibility and data gaps** – In its May 2026 Report on Vulnerabilities in Private Credit, the Financial Stability Board (FSB) highlights uneven regulatory visibility, non-harmonised definitions and limited granular fund- and loan-level information. It is particularly concerned with the ability to identify correlated exposures across complex funding chains.
- **Valuation and price discovery** – Illiquid assets depend more heavily on judgement-based marks. The FCA, FSB and Bank of England are focusing on valuation governance, independence, conflicts, frequency of valuation and whether apparently stable marks could adjust abruptly in stress.
- **Behaviour under system-wide stress** – The Bank of England private-markets SWES is testing how individually rational actions – such as reducing financing, preserving capital, changing allocations or managing redemptions – may amplify or dampen stress across the system and affect the real economy.
- **Evolving Asset Manager regulations** – Divergence between EU AIFMD II and UK AIFM reform proposals will impact larger managers and may require parallel UK and EU compliance approaches. The UK proposals place risk profile, leverage, liquidity, valuation and market impact at the centre of a more proportionate regime, while retaining more detailed requirements for larger or higher-risk managers.
- **Leverage, liquidity and refinancing** – Supervisors are examining leverage at fund and borrower level, liquidity mismatch in redemption-enabled structures, maturity walls and the potential interaction between funding pressure and asset valuations.



What leaders should be thinking about

For boards and executive teams, the practical challenge is to understand where private credit sits within the organisation's strategy and risk profile – whether as borrower, lender, investor, fund manager, insurer, bank counterparty or service provider – and whether governance has kept pace with the market's growth.

- Can we identify our full direct and indirect exposure to private credit across products, legal entities, funds, sponsors and counterparties?
- What is out strategy and corresponding risk appetite for private markets exposures whith clearly defined metric and limits for each relevant segment?
- Are risk appetite and concentration limits keeping pace with growth in NAV lending, subscription finance, warehousing, co-lending and other more complex structures?
- Do valuation governance, collateral monitoring and independent challenge remain robust when observable market prices are limited?
- Are stress tests severe enough to capture correlated borrower weakness, refinancing pressure, valuation adjustments, reduced bank financing and investor liquidity demands occurring together?
- Do senior management and the board receive sufficiently granular information to understand where leverage, liquidity dependencies and concentrations sit across the wider ecosystem?
- Where the organisation is using private credit as a borrower or strategic funding source, are the benefits of speed and flexibility being weighed against cost, covenant, refinancing and lender-control considerations?
- Do our policies, processes and procedures align with private markets-specifics?
- Does our credit risk classification framework tailor for private markets exposures (e.g., including SICR, forbearance, watch-list, UTP policies)?

Private credit: An interconnected web of capital, financing and risk (continued)

Internal Audit considerations

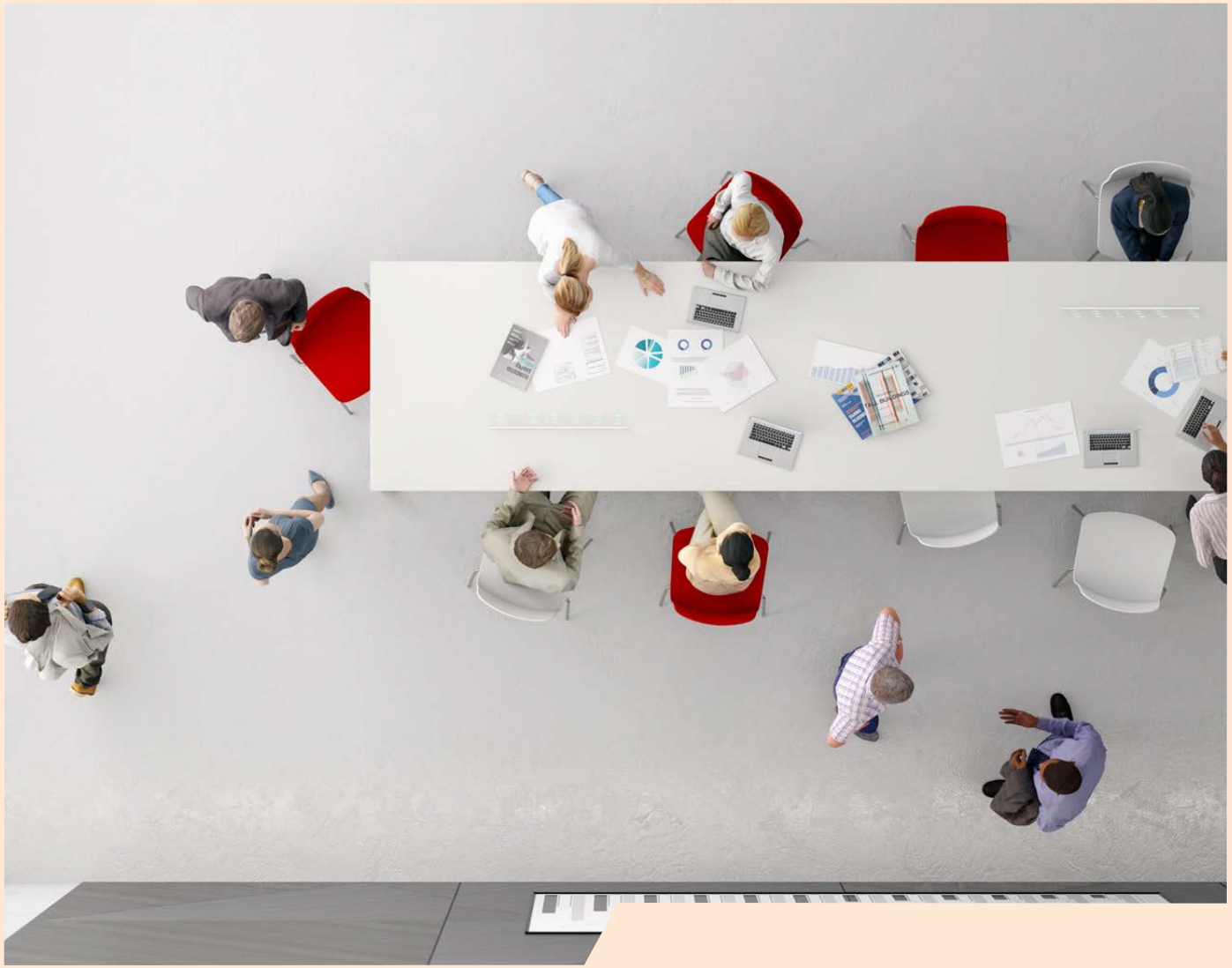
- **Regulatory change and cross-border readiness –** assess whether management has identified the implications of AIFMD II and emerging UK AIFM reforms for relevant funds and managers, including where UK and EU requirements diverge. For firms operating across both regimes, consider whether governance, controls, data and operating models can support parallel requirements without creating gaps, inconsistent standards or unnecessary duplication.
- **Loan-origination and credit-risk controls –** test the design and operating effectiveness of underwriting, borrower assessment, approval, covenant monitoring, ongoing credit review and problem-loan management controls for originated loans, including whether standards remain effective as volumes grow or portfolios move into newer asset classes. Recent market issues have highlighted the need for more robust testing of asset-backed finance portfolio investments including controls over approval of new deals, ongoing monitoring and termination agreements and double-pledging risk.
- **Liquidity, leverage and concentration management –** assess whether limits, monitoring and escalation arrangements appropriately capture fund- and portfolio-level leverage, liquidity mismatch, refinancing dependency and borrower, sponsor, sector or asset concentrations, including under stressed conditions.
- **Valuation governance and challenge –** evaluate whether private-credit valuations are subject to sufficiently independent challenge, supported by appropriate methodologies and data, and responsive to deteriorating credit quality, covenant pressure, refinancing risk and changing market conditions rather than remaining artificially stable.
- **Aggregate exposure and interconnectedness –** assess whether management can identify combined exposures across funds, borrowers, sponsors, financing structures, banks and other counterparties, rather than managing each product or legal entity in isolation.
- **Stress testing and scenario analysis –** challenge whether stress testing captures plausible combinations of borrower deterioration, valuation falls, reduced refinancing availability, investor liquidity pressure and withdrawal of bank or warehouse financing, and whether results lead to credible management actions.
- **Data, MI and regulatory reporting –** test whether management information is complete, timely and sufficiently granular to support risk management, regulatory obligations and Board oversight, particularly where multiple jurisdictions, funds, service providers or legacy systems are involved.
- **Governance and residual risk –** assess whether Boards and senior management receive a transparent view of emerging risks, limit breaches, exceptions, remediation delays and residual exposures.



We have focused this section on a selection of the most topical and significant focus areas and developments that are likely to shape the 2027 agenda. It is not intended to provide an exhaustive view of the risk landscape or audit universe.

Our hot spots include enhancing resilience through establishing a “minimum viable company”, management of external dependency and third-party risk, strengthening cyber security controls, mitigating frontier AI risk and a point of view on Basel 3.1 implementation and T+1 accelerated settlement.

We have included a broader set of sector-specific risk and assurance considerations at the end of the section, highlighting other areas that organisations and Internal Audit functions may wish to keep on their radar as part of 2027 planning.



Risk and regulatory hot spots

Regulatory landscape – the PRA's priorities for banking

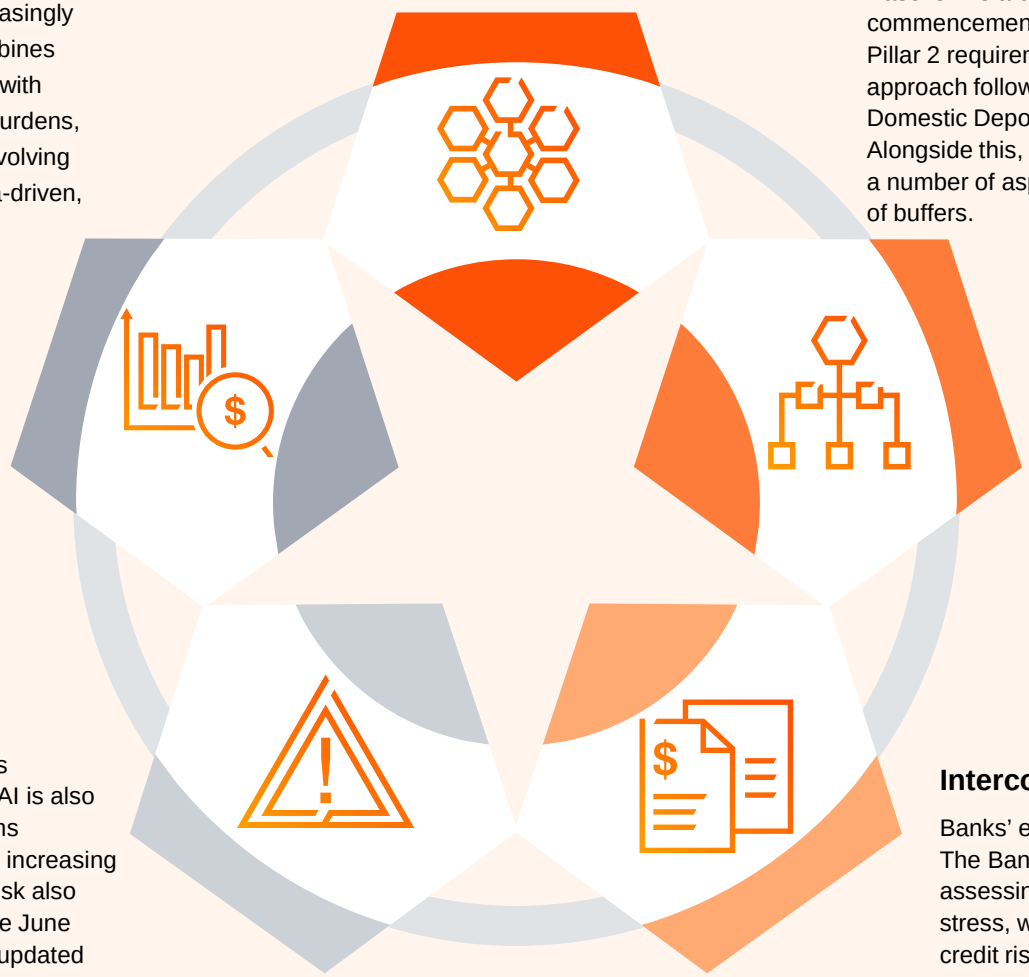
The PRA's 2026/27 agenda remains anchored in the safety and soundness of firms and continuing resilience of the banking sector, while its secondary objectives for international competitiveness and growth are increasingly reflected in policy and regulatory processes. Its programme combines implementation and targeted reform of the prudential framework with greater emphasis on proportionality and reducing unnecessary burdens, while maintaining core prudential standards and responding to evolving risks. Supervision is also being streamlined and made more data-driven, while data risk remains a specific supervisory priority, with focus on data quality, governance and aggregation

Growth, competitiveness and proportionality

The regulatory direction is towards greater proportionality rather than lower standards. This includes Strong and Simple, proposed liquidity-framework modernisation, HMT/PRA ring-fencing reform and continued work on securitisation and the prudential treatment of crypto assets. The consequence for firms is potentially greater flexibility, but also greater reliance on management judgement, governance and evidence that risks remain appropriately identified and controlled.

Emerging and evolving risks

The PRA continues to highlight risks arising from geopolitical, macroeconomic and technological developments, including areas where exposures are complex, fast-growing or less transparent. AI is also attracting increasing supervisory attention: greater use within firms heightens reliance on high-quality data, while frontier models are increasing cyber and operational-resilience risks. Climate-related financial risk also remains part of the supervisory agenda, with firms expected since June 2026 to demonstrate credible plans to address gaps against the updated SS5/25 expectations.



Basel 3.1 and the wider capital framework

Basel 3.1 is a central implementation priority ahead of its 1 January 2027 commencement. The PRA has undertaken off-cycle reviews of firm-specific Pillar 2 requirements ahead of implementation, while the FRTB internal model approach follows in 2028. For smaller domestic banks, changes to the Small Domestic Deposit Takers (SDDT) regime also take effect from January 2027. Alongside this, with the Financial Policy Committee, the PRA is also reviewing a number of aspects of the UK's capital framework, including the useability of buffers.

Operational and third-party resilience

Operational resilience remains a major supervisory priority, with continued focus on firms' testing and their ability to respond and recover effectively from severe disruption, including cyber and third-party incidents. Direct oversight under the Critical Third Parties (CTPs) regime went live in July 2026, with the first four designated technology providers now subject to joint Bank of England, PRA and FCA oversight.

New standardised reporting requirements for operational incidents and material third-party arrangements take effect from March 2027, while SIMEX26 is testing the impact of an extended outage at a major third-party technology provider.

Interconnectedness and non-bank financial institutions

Banks' exposures to NBFIs and private markets remain firmly in focus. The Bank's second system-wide exploratory scenario (SWES) is assessing how banks, insurers and non-banks behave under severe stress, with findings informing future supervisory work on areas including credit risk, model risk and NBFI exposures. The SWES final report is expected in early 2027.

Regulatory landscape – the FCA's priorities for banking



A key feature of the FCA's direction is the move towards a more outcomes-focused, risk-based and data-led supervisory model. Stronger firms may receive less intensive supervision, but greater regulatory flexibility also means greater responsibility for firms to exercise judgement, identify weaknesses themselves and demonstrate that their controls are operating effectively.

Retail banking

Consumer outcomes and Consumer Duty: The FCA is increasingly using firms' data and outcomes monitoring to assess how effectively Consumer Duty is embedded. Particular attention remains on fair value, vulnerable customers and the ability to identify and remediate poor outcomes, with targeted intervention where weaknesses persist. CP26/23 closes on 18 September 2026 and is consulting on targeted changes to the Duty's scope and proportionality, including its application across distribution chains. A policy statement is expected to follow in Q1 2027.

Access to banking and financial inclusion: As banks continue to digitise and, in some cases, reduce physical presence, the FCA remains focused on access to cash and essential banking services, particularly for customers who rely on face-to-face support. Branch closures and digital migration therefore remain important sources of conduct and customer-outcome risk.

Fraud and financial crime: Banks are expected to continually adapt financial-crime controls as criminal techniques and technology evolve. The FCA is increasingly using data and analytics to identify outliers, alongside more targeted engagement with firms with heightened risk or significant control-remediation programmes.

Operational resilience, cyber and data security: Technology transformation, third-party concentration, cyber threats and insider risk remain central concerns. Large-scale technology change programmes are particularly likely to attract scrutiny where weak execution could result in disruption or customer harm. PS26/2 introduces standardised operational-incident and material third-party reporting from 18 March 2027.

Mortgages and responsible innovation: The FCA has consulted on targeted changes to improve mortgage access for creditworthy underserved consumers while retaining affordability requirements, with a policy statement expected by the end of 2026. More broadly, the FCA continues to support responsible adoption of AI and other retail-banking innovations, but expects Consumer Duty, strong governance and controls to remain embedded.

Wholesale markets

Resilience of firms and markets: Areas of attention include trading controls, liquidity management and financial resilience, operational resilience and technology/third-party dependencies, reflecting the potential for weaknesses at individual firms to amplify market stress and disrupt wider market functioning.

Market integrity, financial crime and conduct: Preventing financial crime and market abuse remains a core priority, alongside effective management of conflicts of interest and conduct risk. As markets and technology become more complex, the FCA expects surveillance, data quality, governance and controls to keep pace.

Growth, competitiveness and market reform: Wholesale firms face a significant multi-year transformation agenda covering areas such as listings, securitisation, trading and market transparency, transaction reporting and settlement. New transaction reporting rules were finalised in August 2026, while the UK is moving to T+1 settlement from October 2027. The FCA is seeking simpler and more proportionate regulation while supporting innovation and competitiveness.

Technology and innovation: The FCA is seeking to enable the safe and responsible adoption of AI, digital assets and broader market digitisation, but expects strong governance, testing and controls. Where technology changes trading, surveillance or operations, control frameworks are expected to keep pace with the technology itself.

The Minimum Viable Company: protecting organisational viability through disruption

Does management know what minimum set of outcomes, services and capabilities must keep operating for the organisation to remain viable during severe disruption?

A Minimum Viable Company, or MVC, is the smallest coherent set of critical services and capabilities needed for survival and recovery. It links priority outcomes to the people, processes, technology, data, facilities, suppliers, funding and decisions they depend on.

MVC analysis can be described as identifying the smallest set of critical business services and capabilities essential for survival and recovery.

Why MVC matters

Recent high-impact disruptions have demonstrated how quickly a cyber or operational event can move beyond a technology incident and become an **enterprise viability challenge**. Across sectors, organisations have experienced prolonged loss of digital channels, disruption to production and operations, and knock-on impacts across customers, employees and complex supply chains. These events are testing assumptions embedded in traditional resilience, business continuity and recovery plans – particularly where multiple critical capabilities are unavailable at the same time or recovery takes significantly longer than expected. NCSC guidance now explicitly considers recovery to **minimum viable operations** following highly disruptive incidents.

For financial services firms, this question is especially relevant. FCA/PRA Operational Resilience requirements have driven significant investment in identifying Important Business Services, setting impact tolerances, mapping dependencies and testing resilience.

How organisations should respond

This is bringing Minimum Viable Company (MVC) into sharper focus. MVC asks a different question from whether individual services or processes have continuity plans: **if normal resilience arrangements are overwhelmed, what is the minimum coherent version of the organisation that must continue to operate to preserve viability while wider recovery takes place?** It requires organisations to understand the critical services, internal capabilities, people, technology, data, suppliers and financial resources that must operate together, and to make explicit choices about what must be restored first and what can wait.

For Internal Audit, this creates an important assurance agenda: challenging whether management has identified that minimum operating state, reconciled competing recovery priorities and dependencies, and tested whether it could actually be established and sustained under severe but plausible conditions.



The Minimum Viable Company: protecting organisational viability through disruption (continued)

Resilience is still too often managed through separate disciplines: business continuity, cyber, technology recovery, crisis management, supply-chain resilience and emergency planning. Each may work in isolation, while the organisation still lacks one shared view of what must be protected first.

That fragmentation is becoming harder to defend. The World Economic Forum's outlook to 2028 points to compounding risks, including geoeconomic confrontation, misinformation, cyber insecurity, extreme weather, critical infrastructure disruption and weaponised supply chains. For 2027, the practical implication is concurrent disruption, constrained resources and cascading impacts across organisational boundaries. (World Economic Forum)

Cyber risk illustrates the point. The UK Government's 2025/26 Cyber Security Breaches Survey found that 43% of businesses identified a breach or attack in the previous year, rising to 65% of medium-sized and 69% of large businesses. The NCSC also supported 429 incidents in the year to August 2025, nearly half nationally significant and 18 highly significant. Disruption can no longer be assumed to be exceptional, brief or contained within technology. (GOV.UK)

Board expectations are also tightening. Provision 29 of the UK Corporate Governance Code (where applicable) applies to financial years beginning on or after 1 January 2026 and requires boards to declare the effectiveness of material financial, operational, reporting and compliance controls. Many companies will therefore make their first related disclosures in 2027, supported by evidence from monitoring, review, control weaknesses and near misses. (FRC (Financial Reporting Council))

The MVC provides a practical bridge between enterprise risk, resilience and control. It asks leaders to agree:

01

Which outcomes must continue to protect life, customers, legal and regulatory standing, liquidity, revenue and stakeholder confidence.

02

The minimum acceptable level at which those outcomes can be delivered.

03

Which activities can be stopped, degraded or deferred.

04

The dependencies and vulnerabilities that determine whether the minimum operating state is achievable.

05

The sequence in which scarce recovery resources should be deployed.

This turns resilience from a catalogue of plans into an explicit operating choice owned by management and overseen by the board.

The Minimum Viable Company: protecting organisational viability through disruption (continued)

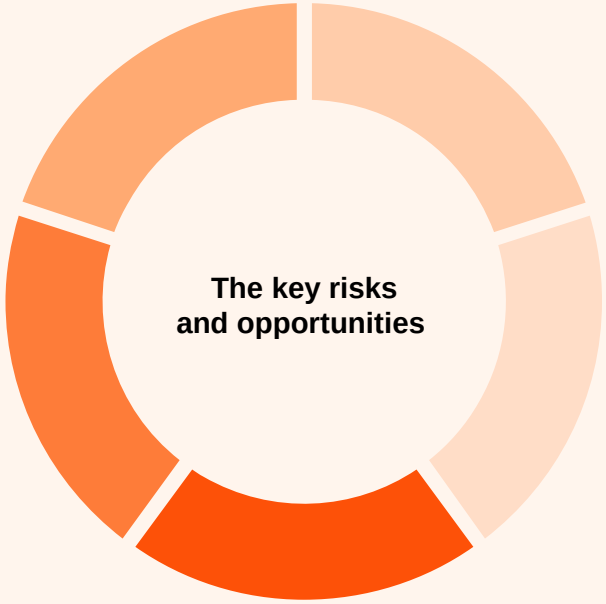
Strategic ambiguity

Without an agreed MVC, functions tend to label their own work as critical. The result is overextended recovery, competing priorities and weak allocation of scarce people, technology, funding or supplier capacity. The opportunity is a board-approved hierarchy of outcomes and tolerances that guides investment, transformation, outsourcing, crisis decisions and recovery sequencing.

Technology-led rather than business-led recovery

Recovery plans often start with applications, platforms and infrastructure because they are tangible. But restoring technology does not automatically restore the business outcome if data, people, suppliers, premises or decision rights are unavailable.

The opportunity is to trace each priority outcome through its full enabling chain: services, activities, information, people, technology, facilities and third parties. FCA observations remain instructive: technology-heavy mapping gives an incomplete resilience view, while clearer ownership and broader dependency mapping improve board challenge and scenario design. (FCA)



Assurance without evidence

Dashboards, policies and recovery-time targets can imply control without proving that priority outcomes can be maintained. An MVC creates an evidence chain from board priorities and risk appetite through dependency mapping, scenario testing, vulnerabilities and funded remediation.

Hidden concentration and common-mode failure

Organisations can look diversified while depending on the same cloud provider, telecoms network, utility, specialist workforce, logistics route or subcontractor. Separate continuity plans may therefore fail together.

An MVC view exposes these concentrations and can shape supplier strategy, architecture, workforce location, insurance, inventory, liquidity and investment before an incident reveals the weakness.

Untested assumptions

Manual workarounds, alternative suppliers, remote working, backup data and reciprocal arrangements often exist on paper but are not tested at the required scale, duration or level of degradation.

The opportunity is to exercise the complete MVC, not isolated response teams. Testing should show whether the minimum operating state can be sustained, where tolerances break and which trade-offs are needed. The UK Government Resilience Action Plan also emphasises training, exercising, governance and frequent board discussion of resilience. (GOV.UK)

The Minimum Viable Company: protecting organisational viability through disruption (continued)



Questions for leaders

01

What is the minimum organisation you need to preserve?

What outcomes, services and capabilities are essential for the organisation to remain viable through a severe and prolonged disruption?

02

What are you prepared to stop or degrade to protect it?

If we cannot maintain everything, have we made the difficult choices about what gets priority, and what can wait?

03

Could you operate that way for a sustained period?

Do you understand how long the organisation could function in a reduced state and the financial, customer, regulatory and operational consequences of doing so?

04

What could prevent you from achieving that minimum state?

Where are the critical dependencies, concentrations or resource conflicts that could undermine your ability to remain viable?

05

Who makes the decisions when normal plans are no longer enough?

Are accountabilities and decision rights clear for prioritising scarce resources, accepting additional risk and changing how the organisation operates?

06

What gives you confidence this will work?

Has the organisation demonstrated through sufficiently severe testing that it could establish and sustain its minimum viable state, rather than relying on individual plans and management assumptions?

The Minimum Viable Company: protecting organisational viability through disruption (continued)



Internal Audit considerations reflecting organisational maturity

01

No formal MVC / early maturity:

Internal Audit should consider whether management has recognised the enterprise viability question at all. Is there a clear understanding of what the organisation would need to preserve if normal resilience and recovery arrangements were overwhelmed?

IA can assess whether existing business continuity, crisis, cyber, recovery and risk frameworks provide a sufficient foundation, and identify gaps where priorities or dependencies remain fragmented.

For regulated FS firms, the starting point should be different: significant foundations may already exist through Important Business Services, impact tolerances, mapping and scenario testing. IA should challenge whether management has used those artefacts to move beyond individual service resilience and consider the minimum combination of IBS, internal enabling capabilities and shared dependencies needed to preserve the firm as a whole.

02

MVC being developed / partially defined:

Where management is starting to define an MVC or equivalent minimum operating model, IA should challenge whether:

- viability outcomes and minimum operating thresholds are clearly defined,
- scope extends beyond customer-facing services to critical internal enablers,
- dependencies, concentrations and resource conflicts are understood,
- priorities and recovery sequencing are enterprise-led,
- governance and decision rights for operating in a degraded state are clear, and
- the approach is integrated with existing Operational Resilience, BCM, cyber, technology recovery, crisis and recovery arrangements.

03

MVC established / more mature:

Where an MVC capability already exists, IA can move from design challenge to operating-effectiveness assurance, considering whether:

- the MVC can actually be established and sustained under severe and prolonged conditions,
- assumptions around data, staffing, suppliers, workarounds, communications and controls have been tested,
- exercises test concurrent failure and resource scarcity rather than validate individual plans,
- vulnerabilities translate into funded, time-bound remediation,
- the construct remains current as the organisation changes, and
- Board reporting distinguishes demonstrated capability from management confidence.

Managing external dependency and third-party risk in 2027

How should financial institutions evolve third-party risk management as reliance on external providers grows, technology adoption accelerates and regulatory expectations continue to increase?

Financial institutions are increasingly dependent on third parties to deliver critical services, technology, data and innovation. Cloud providers, managed services, data providers, AI vendors, financial market infrastructure and specialist suppliers can improve capability and efficiency but also create increasingly interconnected operational and resilience risks.

The question is no longer whether individual suppliers have been appropriately assessed. Firms need to understand how third parties support critical services, where common dependencies and concentrations exist across the portfolio, how risks change throughout the lifecycle and whether disruption can be managed without causing intolerable harm.

Regulatory developments reinforce this direction. The PRA/FCA Material Third-Party reporting regime broadens regulatory visibility beyond traditional outsourcing, while operational resilience, Critical Third-Party and DORA requirements continue to increase expectations around dependency management, resilience, subcontracting and data.

Leading firms are therefore moving third-party risk management (TPRM) from a predominantly onboarding and compliance-led process towards a continuous, data-driven and resilience-focused capability that informs strategic sourcing and risk decisions.

The changing third-party risk landscape

Growing dependency

More critical services depend on cloud, technology, data and specialist external providers

New Technology/AI

Technology is changing the risk perimeter, AI, Cloud and embedded technology services are creating new dependencies faster than traditional TPRM processes can identify and assess them.

Increasing interconnectedness

Fourth parties and shared infrastructure create dependencies that may not be visible through individual supplier assessments.

Faster-changing risk

Cyber, geopolitical, financial, technology and AI risks can change materially between periodic assessments.

Increasing regulatory scrutiny

Regulators increasingly expect firms to demonstrate visibility of material dependencies, credible resilience and exit arrangements, and complete, decision-useful third-party data.



Managing external dependency and third-party risk in 2027 (continued)

How leading financial services firms are adapting

Building a usable third-party universe. 01

Leading firms are consolidating fragmented supplier, contract and service information into a common taxonomy with clear ownership. The objective is not simply to maintain a complete supplier list, but to connect third parties to the services, systems, data, locations and business outcomes they support. This is becoming increasingly important as regulatory and resilience expectations extend beyond traditional outsourcing to a broader range of material third-party dependencies.

Prioritising by criticality and inherent risk. 02

Firms are moving away from spend or organisational profile as proxies for risk and segmenting relationships according to the impact of failure, service criticality, data and technology access, substitutability, regulatory exposure and inherent risk. This enables proportionate due diligence and concentrates specialist challenge on relationships that matter most.

Moving from periodic assessment to continuous monitoring. 03

Initial due diligence remains important, but third-party risks can change materially once a contract is live. Leading firms are moving towards event-driven monitoring, external intelligence and performance data, with clear triggers to identify deterioration and initiate reassessment, escalation or intervention in cyber posture, financial viability, resilience, compliance and service performance.

Integrating TPRM and Operational Resilience. 04

Firms are increasingly connecting TPRM with Operational Resilience to understand which third parties support IBSs/CIFs, identify critical dependencies and test whether disruption can be managed within resilience requirements. This includes greater focus on substitutability, contingency arrangements, supplier participation in scenario testing and credible exit planning.

Understanding fourth parties and concentration. 05

Relationship-level assessments may not reveal where multiple critical services depend on the same cloud provider, technology platform, data provider, subcontractor or specialist workforce. Leading firms are increasingly aggregating relationship, fourth-party and infrastructure dependency data to identify common dependencies, single points of failure and correlated disruption risks.

Do we need assurance? Adapting TPRM for AI, cloud and emerging technology. 06

AI, cloud, data and other emerging services can become critical faster than traditional TPRM processes adapt. Firms are reviewing whether existing due diligence, contracting and monitoring approaches adequately address issues such as data, model risk, explainability, security, resilience, intellectual property and concentration, while avoiding unnecessary barriers to innovation.

Managing external dependency and third-party risk in 2027 (continued)

The key risks and opportunities

Fragmented third-party and dependency data

Disconnected procurement, contract, TPRM, technology and resilience data can prevent firms from understanding which third parties support critical services and where material dependencies exist. The opportunity is to establish a reliable third-party universe with clear ownership, lineage and links to services and dependencies.

01

Point-in-time assurance not keeping pace with changing risk

Due diligence and periodic reassessment provide only a point-in-time view. Cyber, financial, geopolitical, resilience and performance risks can deteriorate rapidly after onboarding. The opportunity is to combine periodic assurance with continuous monitoring, event-driven reassessment and clear intervention triggers.

02

Emerging technology outpacing assurance

AI, cloud and data providers can become material dependencies before traditional assessment methodologies adapt. Firms need assurance approaches that identify material risks across data, models, cyber, resilience, concentration and fourth-party dependencies, while enabling responsible innovation.

03

Concentration hidden below relationship level

Individually acceptable providers depend on common fourth parties, cloud platforms, technology infrastructure, data providers or specialist resources. The opportunity is to define clear processes, roles, responsibilities and the supporting tools to identify, quantify and assess risk concentration so that timely reporting enables informed decisions around substitution, continuity, architecture and strategic sourcing decisions.

04

Fragmented accountability

Procurement, risk, cyber, legal and operational teams may each own part of supplier management without anyone being responsible for the whole risk outcome. The opportunity is to strengthen accountability across the lifecycle: clarifying business ownership, identifying where specialist challenge is needed and determining how material issues should be escalated.

05

Limited substitutability and exit capability

Critical suppliers may be difficult to replace quickly because of data, technology, contractual or market constraints. The opportunity is to assess substitutability earlier, strengthen contingency arrangements and develop credible, tested exit strategies proportionate to criticality.

06

Expanding regulatory perimeter

The expansion from material outsourcing towards broader Material Third-Party reporting increases the importance of complete third-party populations, consistent materiality decisions and high-quality regulatory data. Firms have an opportunity to use regulatory implementation to strengthen the underlying TPRM capability rather than create a standalone reporting process.

07

Managing external dependency and third-party risk in 2027 (continued)



Questions for leaders

- Do we have a complete, consistently classified and decision-useful view of third parties and the critical services, systems and data they support?
- Can we identify common fourth parties and concentrations across cloud, technology, data, infrastructure and other shared providers?
- Are material third-party arrangements beyond traditional outsourcing being consistently identified, assessed and governed?
- Can we detect material changes, incidents and deterioration in critical suppliers early enough to act?
- Are our most critical third-party dependencies supported by credible contingency, substitution and exit arrangements?
- Are AI, cloud and emerging-technology assurance processes keeping pace with business adoption without unnecessarily constraining innovation?
- Can we produce timely, complete and accurate regulatory reporting from our third-party data without significant manual intervention?
- Does Board MI demonstrate whether TPRM is reducing exposure and improving resilience rather than simply showing completion of process activities?

Internal Audit considerations

Internal Audit should move beyond confirming that a TPRM framework exists and determine whether it produces demonstrable risk-management and resilience outcomes. Assurance should focus on whether firms understand their external dependencies, identify changing risks early, make informed risk decisions and can demonstrate that critical services remain resilient when third parties fail. IA should also consider whether TPRM insight is influencing sourcing, resilience, architecture and investment decisions rather than operating primarily as a compliance process.

Third-party universe and data: Completeness, accuracy, classification, ownership and lineage of the third-party population and its linkage to critical services, systems, data and material downstream dependencies.

Continuous monitoring: Whether external intelligence, incidents, performance and other risk signals result in timely reassessment, escalation, intervention and remediation.

Operational Resilience integration: Whether critical third parties are mapped to IBSs/CIFs and appropriately incorporated into resilience testing, substitutability assessments and exit planning.

Regulatory readiness: Whether Material Third-Party populations, materiality decisions, data and reporting processes are ready for the new PRA/FCA regime.

Risk-based lifecycle: Whether materiality, criticality and inherent risk genuinely determine due diligence, contracting, approval, monitoring, reassessment and exit requirements.

Fourth-party and concentration risk: Whether the firm can identify common downstream dependencies and translate concentration insights into sourcing, contingency and resilience decisions.

AI/cloud/emerging technology: Whether assessment methodologies and specialist challenge adequately address emerging technology risks without unnecessarily restricting adoption.

Outcomes and MI: Whether management information demonstrates reduced exposure, timely remediation, tested resilience and improved decision-making rather than process completion alone.

Managing external dependency and third-party risk in 2027 (continued)

Connecting TPRM, Operational Resilience and Strategic Sourcing

TPRM should not operate in isolation. Procurement and Strategic Sourcing determine which external capabilities the firm acquires, TPRM assesses and monitors the risks arising from those relationships. Operational Resilience considers how critical dependencies affect the firm's ability to continue delivering important services during disruption.

Leading firms connect these perspectives so that supplier-level information informs portfolio-level concentration and resilience decisions, while resilience insights influence sourcing, contracting, monitoring and exit decisions.

For Internal Audit, the implication is equally practical. Assurance should not only assess whether each framework operates independently, but whether information flows effectively between them and changes management decisions.

The key question is whether the organisation can move from:

supplier → service → dependency → business impact → management action.

Where that chain is incomplete, material third-party, concentration and resilience risks can remain hidden even where the individual TPRM, sourcing and Operational Resilience frameworks appear mature. The leading question for 2027 is therefore not whether each discipline is mature in isolation, but whether together they provide a decision-useful view of the firm's external dependencies and resilience.



The changing shape of cyber risk – what leaders need to act now on



Cyber security is no longer principally an IT issue managed behind the scenes. It increasingly affects physical safety, service continuity, public trust and the confidence of investors, regulators, customers and supply chain partners. Three developments demand attention: the growing connectivity of operational technology and critical infrastructure, rising scrutiny of third-party, supplier and concentration risk from all directions. the emerging threat that quantum computing poses to the cryptography underpinning digital trust. Alongside these, AI is altering both the threat environment and the tools available to defenders – raising the pace, scale and sophistication on both sides. Internal Audit should assess whether these exposures are understood, owned and managed within risk appetite.



Why the topic matters in 2027

Connected operations, physical consequences

Operational technology is moving from isolated engineering environments into connected digital ecosystems. Industrial control systems, sensors, remote access tools and cloud-enabled monitoring are creating new routes into the processes that keep organisations, communities and infrastructure running. Manufacturing was the most attacked sector globally in 2025 for the fifth consecutive year, absorbing 27.7% of all cyberattacks tracked by IBM X-Force. But this is not confined to heavy industry. Building management systems – the platforms that run HVAC, lighting, access control and fire safety – sit inside almost every organisation with a physical estate. Research from Claroty found that 75% of organisations have building management systems affected by known exploitable vulnerabilities, and 69% of those have devices with vulnerabilities already linked to ransomware. A compromised building management system can be as effective an entry point into a corporate network as any factory floor.

The defining feature of operational technology risk is consequence. A compromised controller, workstation or monitoring tool can halt production, disable safety systems, disrupt environmental controls and force manual workarounds under pressure. Connectivity brings efficiency – but it also gives cyber incidents a direct route into physical operations.

Rising demand for cyber assurance across supply chains and stakeholders

The focus on cyber security is no longer driven solely by those buying or selling businesses. Customers, regulators, investors and supply chain partners are all asking harder questions about how organisations protect data, maintain service continuity and manage the third parties they depend on. Concentration risk – where multiple critical services rely on the same cloud provider, managed service provider or specialist vendor – can create common points of failure that affect entire sectors. A single supplier incident can cascade across organisations that believed their risk was diversified.

This scrutiny is increasing from all angles. Regulators are tightening expectations around operational resilience and third-party oversight. Large customers increasingly require evidence of cyber maturity as a condition of doing business. Investors – whether at the point of acquisition, IPO or ongoing stewardship – expect governance, incident discipline and disclosure readiness to be demonstrable, not merely asserted. Organisations that treat cyber as an always-on capability – with consistent baselines, tested response arrangements and a clear view of their supplier dependencies – are better positioned for growth, partnership and public trust. Those that cannot evidence their posture face delayed transactions, lost contracts, regulatory challenge and reputational harm.

The changing shape of cyber risk – what leaders need to act now on (continued)

The quantum threat to cryptography

Quantum computing poses a fundamental, longer-term challenge to the public-key cryptography that protects nearly all digital communication, authentication, data storage and software integrity today. The threat is not theoretical: the NCSC has stated that large quantum computers will be able to break current public-key algorithms and has set out a clear timeline for UK organisations to migrate to post-quantum cryptography (PQC), with initial high-risk system discovery by 2028, priority migrations complete by 2031 and full migration by 2035.

The immediate risk is 'harvest now, decrypt later' – where adversaries intercept and store encrypted data today, intending to decrypt it once quantum capability matures. Data that must remain confidential for years or decades – government communications, health records, intellectual property, financial data, legal privilege – is already at risk if protected only by algorithms that quantum computers will break.

Migration will not be straightforward. Cryptography is deeply embedded across certificates, identity infrastructure, VPNs, software signing, payment systems, IoT devices and operational technology. The NCSC's guidance emphasises that organisations should begin now with discovery – understanding where vulnerable cryptography is used and which systems carry the greatest sensitivity or longest data life. Organisations that delay discovery will face compressed migration timelines, higher costs and a greater risk of disruption when change eventually becomes unavoidable.

The US National Institute of Standards and Technology (NIST) published its first post-quantum cryptographic standards in 2024. Vendors are beginning to build PQC into products and services, but readiness varies significantly. Organisations should align migration planning to vendor roadmaps, relevant standards and the NCSC's phased timeline – prioritising systems that protect long-life sensitive data and those that support critical infrastructure or supply chain trust.

AI is changing the threat landscape

AI, and specifically 'Frontier AI', the most advanced tools and models available, is making attacks faster, more targeted and harder to detect. Threat actors are using generative AI to craft more convincing phishing, to automate reconnaissance and to accelerate the development of novel malware. Autonomous 'agentic' systems can probe networks, adapt in real time and operate at a speed that outpaces traditional monitoring. On the defensive side, AI is increasingly embedded in detection, triage and response tooling – but its effectiveness depends on the quality of data, the clarity of its decision authority and the human oversight surrounding it. Where AI is used in cyber defence, organisations need to understand what it can access, what actions it can take autonomously and what happens when it gets things wrong.



The changing shape of cyber risk – what leaders need to act now on (continued)

The key risks and opportunities

Old assets, new exposure

Many operational technology environments depend on long-life assets built for stability, not connectivity. Remote access, supplier links and information technology-operational technology convergence now extend those assets into threat environments they were never designed for. The opportunity is to make the invisible visible: clearer asset inventories, stronger segmentation, tighter access controls and safer remote support – delivered in a way that protects operational uptime rather than hindering it.

01

Privileged access beyond the perimeter

Engineering partners, equipment manufacturers and managed service providers often hold the keys to OT environments and critical systems. Their access is essential but can become a direct route into critical processes if poorly governed. More broadly, supply chain partners, cloud providers and specialist vendors hold privileged positions across the digital estate. The opportunity is to treat third-party access as an operational resilience control – with approval, monitoring, incident notification, continuity expectations and joint recovery arrangements – regardless of whether the system is IT or OT.

02

Concentration risk hiding in plain sight

Organisations may believe their risk is diversified while relying on the same providers across multiple critical services. A single cloud outage, vendor compromise or geopolitical disruption can affect several business processes simultaneously. The opportunity is to map material dependencies, understand where common points of failure exist, set proportionate resilience requirements and maintain credible continuity and exit arrangements.

03

AI-enabled threats outpacing static defences

AI allows threat actors to operate at machine speed – automating social engineering, vulnerability exploitation and lateral movement. Organisations relying on static, rule-based defences face a growing gap. The opportunity is to ensure that detection, monitoring and response arrangements reflect the current threat environment, with clear governance over AI-enabled defensive tools, including what they can access and do autonomously.

04

Cryptographic debt accumulating silently

Data encrypted today may remain sensitive for decades. Organisations that have not begun cryptographic discovery are accumulating risk they cannot yet see. Certificates, identity systems, VPNs, software signing and device authentication all depend on algorithms that will eventually need replacing. The opportunity is to start now: identify where vulnerable cryptography protects long-life data or critical infrastructure, classify systems by sensitivity and migration complexity, and develop a phased plan aligned to NCSC timelines and vendor readiness – before the migration window compresses.

05

The changing shape of cyber risk – what leaders need to act now on (continued)



Questions for leaders

What really keeps the operation running – and can we evidence its resilience? Which sites, assets and physical processes are essential to safe, compliant and continuous delivery, and is there enterprise-level proof that they can withstand a severe cyber incident?

Where does the outside world connect? How are operational technology environments, corporate networks and critical systems separated from supplier networks, cloud services and remote support channels?

Who can make the hard call? Are decision rights clear for isolating systems, stopping production or moving to manual operations during an incident?

Do we understand our concentration risk? Which providers and suppliers support multiple critical services, and are continuity and exit arrangements credible if one fails?

What do our customers, investors and regulators expect us to evidence – and can we? Would governance, incident materiality and disclosure controls withstand external scrutiny today?

Are third parties held to the same standard? Is supplier access approved, monitored, reviewed and tested with the same rigour applied to internal privileged access?

How is AI changing the threats we face – and the defences we rely on? Do detection and response capabilities reflect the speed and sophistication of AI-enabled attacks, and is human oversight maintained over autonomous defensive tools?

Have we started our quantum migration? Has the organisation identified long-life sensitive data, mapped where vulnerable cryptography sits across systems and supply chains, and set a phased migration approach aligned to NCSC guidance?

Internal Audit considerations

These areas span different time horizons – operational technology resilience and supply chain assurance require action now, quantum migration demands planning now and execution over the coming years – but they should be assessed through a common lens: is the organisation keeping pace with the exposure its own operations, dependencies and data create?

Internal Audit should test whether:

The OT asset inventory is complete and risk-ranked, showing what is critical, what is unsupported and what has been genuinely reviewed recently.	Segmentation, remote access controls and monitoring operate as designed across critical OT and IT environments in daily practice – not just on paper.
Incident response plans address safety, environmental controls and manual workarounds alongside technical recovery, with decision rights clearly assigned.	Ownership and escalation routes are understood across operations, engineering, cyber, safety, crisis management and third-party management.
Material supplier and provider dependencies are mapped, with resilience requirements, incident arrangements and credible fallback or exit options in place.	Concentration risk is visible at enterprise level – showing where common providers, platforms or access routes create shared points of failure.
Third-party access to critical environments is approved, monitored and reviewed with rigour proportionate to the access granted.	The organisation's view of the threat landscape reflects the impact of AI on attack methods, and detection and response capabilities are tested against realistic, current scenarios.

The changing shape of cyber risk – what leaders need to act now on (continued)

Internal Audit considerations (continued)

Long-life sensitive data and material cryptographic dependencies have been identified, with a discovery exercise completed or under way in line with NCSC's recommended timelines.

Migration priorities are set by reference to data sensitivity, system criticality, vendor readiness and the time needed to replace certificates, identity infrastructure and embedded cryptography.

Exercises bring together site teams, engineering, central functions, suppliers and leadership – and findings are translated into owned, funded and retested improvements.

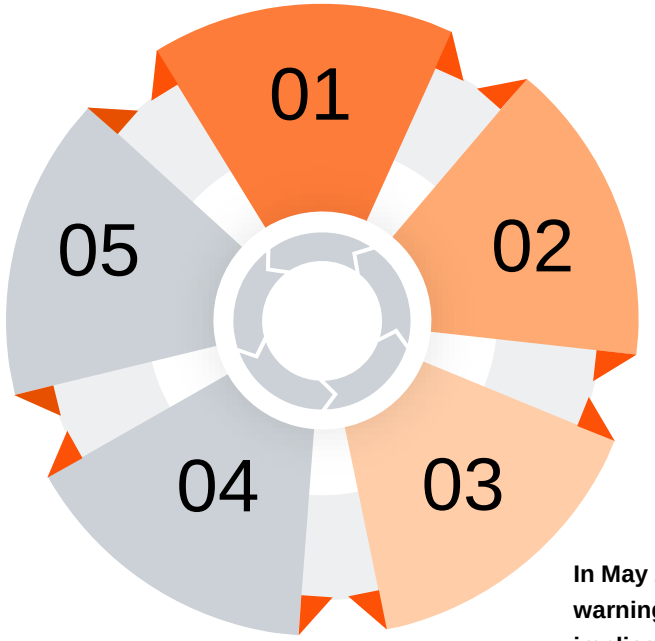
Policies, architecture diagrams and supplier assessments demonstrate control design but do not prove operational effectiveness. Internal Audit should test whether controls work under pressure – whether segmentation holds, supplier access is genuinely monitored, exercises prove recovery within agreed tolerances and cryptographic discovery is producing actionable results. Findings should set out the affected business service, the potential impact, the control weakness and the accountable risk owner.



Frontier AI: keeping pace with accelerating threats

Frontier AI refers to the most capable AI models available at a given point in time. Their capabilities are evolving rapidly and can subsequently be transferred into smaller, cheaper or open-weight models, meaning advances at the frontier can quickly influence the wider AI ecosystem. Increasingly, these models are also being incorporated into agentic systems that can plan, make decisions and take sequences of actions with limited human intervention.

The message to regulated firms is therefore one of preparedness rather than waiting for the threat to mature. The authorities expect firms and financial market infrastructures to plan for and mitigate frontier AI-related cyber risks through their existing operational resilience and cyber frameworks. Importantly, the statement does not introduce new regulatory expectations, rather, it reinforces existing expectations in light of a faster and more complex operating environment.



For financial services firms, the immediate concern is their impact on cyber risk and operational resilience. Frontier AI does not fundamentally create an entirely new category of cyber threat, instead, it can materially increase the speed, scale and affordability with which existing weaknesses are identified and exploited. Tasks that previously required specialist skills — including understanding system architecture, identifying vulnerabilities and developing elements of attacks — can increasingly be automated. The NCSC notes that in certain cyber tasks, frontier models already exceed the capabilities of skilled practitioners while operating at lower cost.

There is also an important defensive dimension. The NCSC expects AI ultimately to be a net positive for cyber security if defenders adopt it effectively. AI can potentially accelerate vulnerability discovery, improve threat detection and investigation, and enable faster containment and remediation. The challenge for firms will therefore be to retain a defensive advantage by strengthening cyber fundamentals while safely exploiting AI-enabled defensive capabilities.

In May 2026, the Bank of England, FCA and HM Treasury issued a joint statement warning that frontier AI represents a step-change in capability with significant implications for cyber security and operational resilience. The authorities highlighted the potential implications for firms' safety and soundness, customers, market integrity and ultimately financial stability. They expect the risks to increase as more capable models become available and warn that firms that have underinvested in basic cyber security are likely to become progressively more exposed.

Frontier AI: keeping pace with accelerating threats (continued)

Key risks and opportunities

- **Accelerated cyber threats**: Frontier AI can increase the speed, scale and affordability of cyber attacks, enabling vulnerabilities to be identified and exploited more quickly and lowering the level of specialist expertise required.
- **Legacy and accepted risks become more exposed:** Unsupported technology, incomplete asset inventories and longstanding control weaknesses may become materially more difficult to tolerate as AI reduces the time and expertise needed to exploit them. Firms may need to reassess whether historic risk acceptances and remediation timelines remain credible in the changed threat environment.
- **Remediation capacity becomes the constraint:** As AI increases the pace and volume of vulnerability discovery, the challenge may shift from finding weaknesses to validating, prioritising and fixing them. Traditional severity- and SLA-based approaches may need to give greater weight to exploitability, exposure and business criticality, while growing remediation backlogs could place significant pressure on engineering capacity.
- **Third-party and supply-chain concentration:** Dependencies on outsourced providers, software libraries and open-source components may create additional exposure where vulnerabilities can be identified and exploited rapidly across multiple firms.
- **Faster-moving operational disruption:** More automated attacks could reduce the time available for detection, containment and recovery, increasing the importance of effective monitoring and operational resilience.
- **Opportunity to strengthen cyber defence:** Frontier AI can also improve vulnerability discovery, threat intelligence, alert triage, investigation and remediation, potentially allowing defenders to respond more quickly and effectively.
- **Greater automation of security operations:** AI may enable more continuous security testing and, over time, greater automation of containment and remediation. This could improve efficiency, but incorrect automated actions could themselves create operational disruption.
- **Potential for a defensive advantage:** Firms that combine strong cyber fundamentals with effective adoption of AI-enabled defensive tools may be better placed to keep pace with evolving attacker capabilities.



Frontier AI: keeping pace with accelerating threats (continued)

Questions for leaders

01

Do we understand where frontier AI materially changes our cyber risk profile?

02

Are our cyber fundamentals strong enough to withstand vulnerabilities being identified and exploited at greater speed and scale?

03

Where are our most significant legacy, unsupported or poorly controlled technology exposures?

04

Can our vulnerability-management processes respond quickly enough to a significant increase in vulnerabilities?

05

Do we understand our exposure through third parties, software dependencies and open-source components?

06

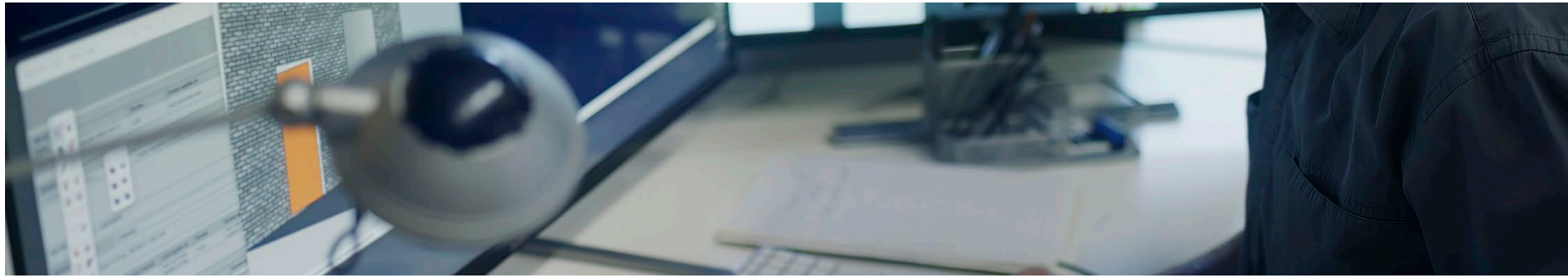
Are our detection, response and recovery capabilities fast enough for AI-enabled attacks?

07

Are we using AI effectively to strengthen cyber defence while managing the risks it introduces?

08

Do our investment, skills and resilience-testing programmes reflect the changing threat environment?



Frontier AI: keeping pace with accelerating threats (continued)

Internal Audit considerations

Internal Audit should consider whether existing cyber assurance remains appropriate as Frontier AI increases the speed, scale and affordability with which vulnerabilities can be identified and exploited.

Risk assessment and governance
Assess whether the implications of Frontier AI for the firm's cyber risk profile are understood by senior management and appropriately reflected in cyber and operational resilience governance.

Cyber control environment
Assess whether foundational controls remain effective as Frontier AI increases the speed and scale at which weaknesses can be identified and exploited, with particular focus on asset management, identity and access, secure configuration, logging, monitoring and legacy technology.

Vulnerability management and remediation capacity
Assess whether vulnerability identification, validation, prioritisation and remediation can operate at the speed and scale required, including whether engineering capacity and remediation backlogs constrain the firm's ability to respond.

Third-party dependency risk
Evaluate whether the firm has sufficient visibility of critical technology, software and open-source dependencies, and whether supplier vulnerability and incident-management arrangements support rapid response.

Detection, response and operational resilience
Review whether monitoring, containment, recovery and resilience arrangements remain effective under faster AI-enabled attack scenarios, and whether identified weaknesses translate into timely remediation.

AI-enabled defensive tooling
Where AI is used in cyber defence, assess governance, human oversight, access permissions and the consequences of incorrect or autonomous actions.

Internal Audit capability
Consider whether Internal Audit has sufficient cyber and AI expertise to challenge the evolving risk and whether targeted or thematic assurance is required as Frontier AI capabilities develop.



PS26/2: Operational incident and third-party reporting

Following consultations in 2024, the FCA and PRA confirmed final rules and guidance which set out the requirements for operational incident and third-party reporting. These rules will apply to in-scope firms from 18 March 2027. While the final rules are a simplification of the reporting framework, they will require firms to act and report with greater speed.

Operational incident reporting

For in-scope firms, incidents that meet a notification threshold must be reported, namely incidents that pose a risk to:

- Consumer harm from which consumers cannot easily recover
- Safety and soundness of the firm and/or market participants
- Market stability, market integrity or confidence in the UK financial system.

As recently re-emphasised by regulators, the new requirements regarding incident reporting should not require a wholesale change/rebuild of incident and resilience frameworks. While the operational incidents to be reported are not limited to those impacting an IBS, or breaching an impact tolerance, the mapping and data points used by firms from their work on IBS (and DORA) can be used to inform impacts and threshold assessments. Incorporating the reportability decision-making process into scenario, crisis and incident testing is key to pressure testing a firm's approach to incident reporting and identifying any weaknesses, gaps or lessons learned.

For banks and other enhanced-reporting firms, the initial incident report must be submitted as soon as practicable and is expected within 24 hours of determining that a threshold has been met, it must then be updated for significant changes and finalised within 30 working days of resolution, or no later than 60 working days where the shorter period is impracticable. Dual-regulated firms make one report through FCA Connect, selecting the relevant regulator or regulators.

Third-party arrangements

Under the new regime, in-scope firms will be required to notify the regulators when entering into, or making a significant change to, a Material Third-Party (MTP) arrangement and maintain and submit an annual register of their MTP arrangements. Importantly, the regime extends beyond traditional material outsourcing to include material non-outsourcing third-party arrangements, significantly broadening the population firms need to assess.

The requirements place increased importance on the completeness and quality of third-party data. Firms will need to understand their third-party population beyond outsourcing, establish clear ownership and governance over materiality decisions, identify significant changes requiring notification, and maintain sufficiently complete and accurate information to support both event-driven notifications and annual regulatory submissions.

Determining materiality remains the firm's responsibility. Firms will need a robust and consistently applied methodology for identifying MTP arrangements, considering whether disruption or failure could cause intolerable client harm, threaten the firm's ability to meet regulatory obligations or operational resilience requirements, or pose risks to the soundness, stability, resilience, confidence or integrity of the UK financial system.

Existing senior management accountability for outsourcing remains relevant, while MTP reporting will require clear governance and accountability for determining materiality, approving arrangements and ensuring accurate and timely regulatory reporting.



PS26/2: Operational incident and third-party reporting (continued)

Key considerations for firms

Firms should focus on building a single, integrated operating model for incident and third-party reporting. This should clearly define how incidents are identified, assessed and escalated, who determines reportability, when the reporting clock starts and who has authority to approve and submit reports, including outside normal business hours.

Data quality and availability will be critical. Firms need timely information on affected systems, services, customers, legal entities and third parties to support threshold assessments and regulatory submissions. Existing operational resilience mapping and incident data should be reviewed to confirm that they provide sufficient evidence during a live event.

Establish clear data ownership and end-to-end data lineage across Third-Party Risk Management (TPRM), Procurement, Technology, Operational Resilience, and business functions to enable complete, accurate, and timely regulatory submissions.

Conduct pre-implementation testing of Material Third-Party (MTP) notifications and annual register production to identify gaps in population completeness, data availability, governance arrangements and reporting processes.

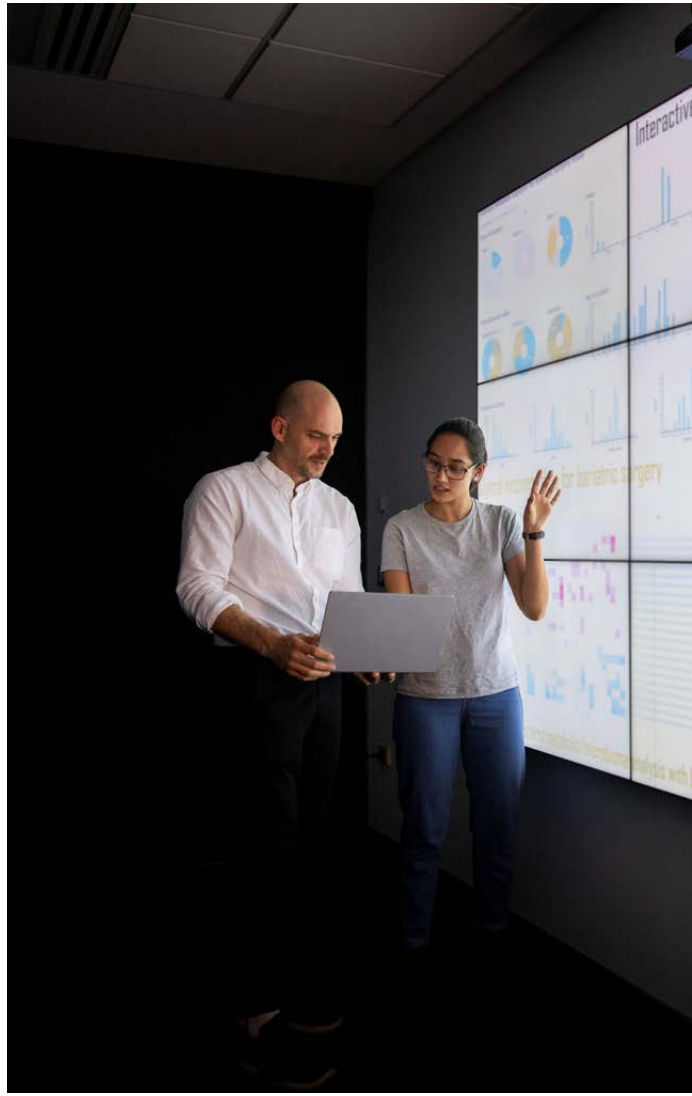
Reportability should also be tested through scenario exercises. Firms should assess whether they can obtain the necessary information, apply judgement, secure approvals and meet reporting deadlines without distracting teams from containment and recovery.

For third-party reporting, firms should ensure that their material third-party population is complete and extends beyond traditional outsourcing. Procurement, contract, cloud, service-mapping and third-party risk data may need to be reconciled to identify material outsourcing and non-outsourcing arrangements and establish a reliable regulatory reporting population.

Ensure clear senior management accountability for MTP reporting obligations, while maintaining the required allocation of the PRA Prescribed Responsibility for outsourcing obligations, where applicable.

Materiality and significant-change assessments should be embedded throughout the third-party lifecycle, including onboarding, renewal, material service change, migration and exit. Supporting contractual arrangements should enable timely access to relevant information, including incidents, recovery, root-cause analysis and subcontractor dependencies, where appropriate.

Finally, firms should coordinate the new regime with existing regulatory, legal, customer and contractual notification obligations. Implementation should result in a sustainable business-as-usual process, supported by clear ownership, appropriate governance and MI, periodic testing and lessons learned from incidents and reporting exercises.



PS26/2: Operational incident and third-party reporting (continued)



Questions for leaders

01

Can we determine and evidence, within hours, whether an incident meets the FCA threshold, the PRA threshold or both – including where several events are linked?

02

Who has authority to make the reporting decision and submit or update the report 24/7, and is there a tested deputy and escalation route?

03

Do our severity ratings, cyber classifications, consumer-harm assessments, prudential triggers, important business services and impact tolerances lead to a consistent reporting outcome?

04

Have we established which operational incident and Material Third-Party reporting requirements apply to each relevant legal entity, including the applicable reporting classification and regulatory reporting route?

05

Are we confident that our Material Third-Party population is complete, including material non-outsourcing arrangements and relevant dependencies, and that ownership and lineage are established for the data required to support regulatory reporting?

06

Can we identify when a third-party arrangement becomes material, or when a change to an existing arrangement becomes sufficiently significant to trigger regulatory notification?

07

Do we know where the required regulatory reporting data resides, who owns it and whether we can produce a complete and accurate MTP register without significant manual intervention?

08

Do our contractual and operational arrangements provide timely access to the third-party incident, recovery, root-cause and subcontractor information required to support regulatory reporting and effective risk management?

09

Does Board and executive MI provide sufficient visibility of material third-party dependencies, concentration and resilience risks, reportable incidents, threshold decisions and remediation activity to support effective challenge and investment decisions?

10

Have we performed end-to-end dry runs of both operational incident and Material Third-Party reporting to demonstrate that our data, technology, governance and people can meet the new requirements under realistic conditions?

12

How do Critical Third-Party (CTP) designations affect our understanding of concentration, substitutability, resilience testing and exit planning, while recognising that accountability for managing third-party risk remains with the firm?

PS26/2: Operational incident and third-party reporting (continued)

Internal Audit considerations

Governance, scope and implementation readiness:

Assess whether the regulatory interpretation, legal-entity scope and target operating model are clear and appropriately governed, with defined senior management accountability, decision rights and first- and second-line responsibilities. Test whether implementation plans address key dependencies, data remediation, technology changes, training, dry runs and go-live criteria, with material risks and delays appropriately escalated.

Incident identification, assessment and reporting:

Test the end-to-end incident reporting process through severe but plausible scenarios, from detection and linked-event aggregation through threshold assessment, escalation, regulatory submission, updates and final reporting. Review reported and unreported incidents, including near misses, to assess the consistency, quality and evidencing of reporting decisions, including where incidents do not affect an important business service. Assess whether containment and regulatory reporting can operate effectively in parallel.

Material third-party reporting and data:

Assess the completeness and accuracy of the Material Third-Party population and application of materiality criteria, including relevant non-outsourcing arrangements. Trace key regulatory data from authoritative source systems through to notifications and the annual register, testing data ownership, lineage and controls for identifying new or significantly changed arrangements. Assess whether contractual and operational arrangements provide timely access to incident, subcontractor and other information needed to meet reporting obligations.

Operating effectiveness, integration and oversight:

Assess whether incident management, operational resilience, third-party risk management and regulatory reporting operate as an integrated framework rather than disconnected processes. Evaluate whether management information supports effective Board and executive challenge and provides visibility of decisions, ownership, investment and overdue remediation. Internal Audit should adopt a phased assurance approach, testing readiness before go-live and undertaking post-implementation assurance in 2027 using actual submissions, regulator feedback, data-quality exceptions and lessons learned to determine whether the operating model is embedded and sustainable.



Implementation of Basel 3.1, Small Domestic Deposit Takers (SDDT) and operational resilience requirements

For UK banks and building societies, 2027 represents a significant milestone in the prudential and operational resilience agenda. The implementation of Basel 3.1 and the SDDT framework from 1 January 2027, together with the introduction of new operational incident and material third-party reporting requirements from 18 March 2027, will require firms to demonstrate that these significant regulatory changes have been fully embedded into business-as-usual operations.

The reforms extend beyond compliance with new rules. Basel 3.1 introduces fundamental changes to the calculation of capital requirements, risk-weighted assets, regulatory reporting and disclosures, while the SDDT framework provides eligible smaller firms with a simplified prudential regime. Beyond regulatory compliance, Basel 3.1 is expected to reshape firms' approaches to capital allocation, risk appetite, pricing and portfolio strategy. The reforms may alter the relative attractiveness of different products and customer segments, requiring firms to reassess how capital is deployed while maintaining competitiveness and profitability. At the same time, regulators expect firms to demonstrate mature operational resilience capabilities, supported by effective governance, reliable data, robust incident management and comprehensive oversight of third-party dependencies.

For many firms, the changes will go live alongside wider transformation programmes, increasing implementation risk and placing greater reliance on data quality, systems, governance and effective change management. Boards should therefore expect supervisory attention to focus not only on technical compliance but also on whether firms can evidence sustainable operational capability, effective oversight and informed decision-making. For firms using internal models, implementation will also require parallel standardised capital calculations to support compliance with the output floor requirements, creating additional reporting complexity and increasing the importance of integrated governance across Risk, Finance and Technology functions.



Implementation of Basel 3.1, Small Domestic Deposit Takers (SDDT) and operational resilience requirements (continued)

Key considerations for firms

By 2027, firms should be demonstrating that Basel 3.1 or the SDDT framework and enhanced operational resilience requirements have been embedded into business-as-usual governance, operating models and decision-making. While regulatory compliance remains essential, firms should also view these reforms as an opportunity to strengthen resilience, potentially rebalance portfolio mix, improve profitability, improve decision-making and enhance long-term competitiveness through coordinated action across Risk, Finance, Technology and Operations.

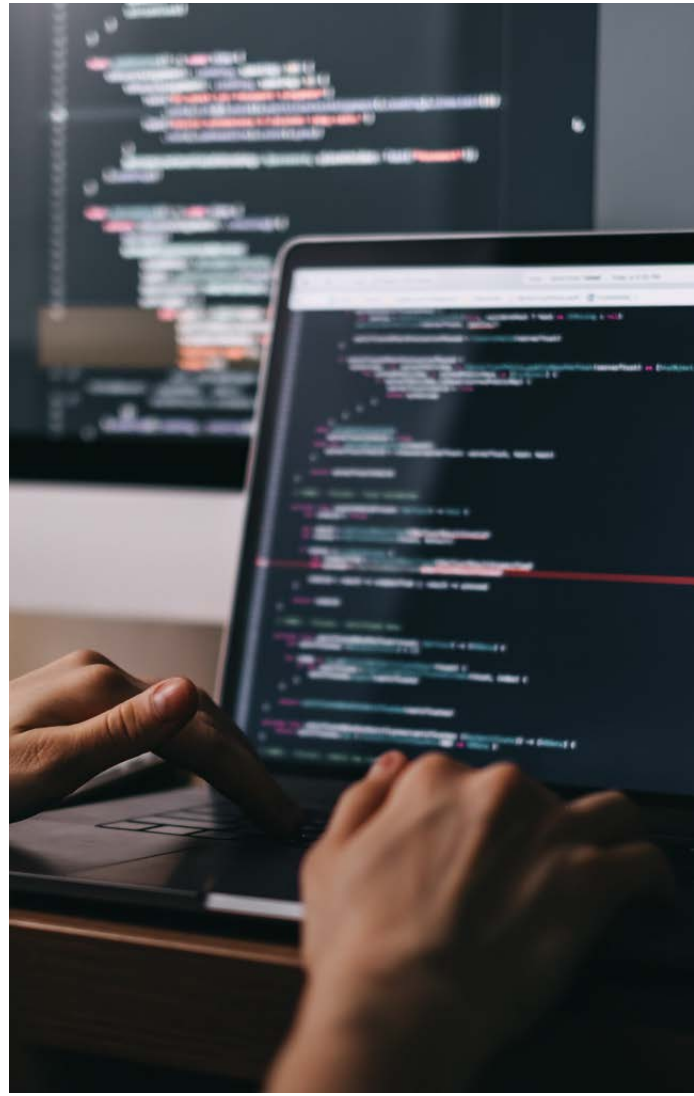
Delivering multiple regulatory reforms alongside wider transformation programmes increases the risk of implementation delays, resource constraints and control weaknesses. Firms should therefore adopt an integrated approach to regulatory change, ensuring implementation risks and interdependencies are actively managed through effective governance and Board oversight. Done well, this can strengthen programme governance and improve the organisation's ability to respond to future regulatory change.

Basel 3.1 has implications that extend beyond regulatory capital calculations and may materially influence capital allocation, product profitability, pricing, lending decisions and overall business strategy. Firms that focus solely on achieving compliance risk overlooking the broader commercial impact of the reforms and falling behind peers. Instead, firms should assess how changes to risk-weighted assets affect their business model, risk appetite and portfolio strategy. A more strategic assessment can support optimisation of capital, improve pricing decisions and enable firms to allocate capital more efficiently while maintaining competitiveness.

The reforms also place greater reliance on robust data, effective governance and accurate regulatory reporting. Weak data quality or fragmented reporting processes increase the risk of inaccurate regulatory submissions, particularly where firms must support parallel reporting requirements under the output floor. Investment in data architecture, automation and reporting controls presents an opportunity to improve regulatory compliance while strengthening management information and business decision-making.

Operational resilience requirements continue to evolve beyond implementation, with regulators expecting firms to demonstrate resilience through ongoing testing, remediation and continuous improvement. Concurrently, enhanced operational incident and third-party reporting requirements reinforce the need for effective governance over critical services and external dependencies. Aligning operational resilience, incident management and third-party risk management can strengthen enterprise resilience while providing Boards with more integrated oversight of operational risk.

Ultimately, firms should focus not only on achieving technical compliance but on embedding these reforms into sustainable business operations. Strong cross-functional collaboration, clear accountability and integrated governance will help ensure the changes deliver lasting improvements in resilience, operational effectiveness and strategic decision-making.



Implementation of Basel 3.1, Small Domestic Deposit Takers (SDDT) and operational resilience requirements



Questions for leaders

01

Do we clearly understand how Basel 3.1 or the SDDT framework will affect our capital position, business model and strategic objectives?

02

Have implementation programmes moved beyond regulatory interpretation into sustainable business-as-usual operating models, controls and governance?

03

Are our regulatory reporting processes supported by sufficiently robust data governance, systems and controls?

04

Can we demonstrate that important business services remain within approved impact tolerances during severe but plausible disruption?

05

Do we have clear governance for identifying, escalating and reporting operational incidents under the new regulatory requirements?

06

Is our inventory of material third-party arrangements complete, accurate and supported by appropriate governance and ownership?

07

Have we assessed the cumulative risks associated with delivering multiple regulatory change programmes simultaneously?

08

Does the Board receive sufficiently integrated management information to oversee prudential, operational resilience and third-party risks?

09

Have we assessed whether Basel 3.1 requires changes to our risk appetite, product pricing or portfolio strategy?

10

Do our Risk, Finance and Technology functions have the capabilities, governance and data required to support new capital calculations and regulatory reporting on a sustainable basis?

Implementation of Basel 3.1, Small Domestic Deposit Takers (SDDT) and operational resilience requirements (continued)

Internal Audit considerations

Internal Audit has an opportunity to provide independent assurance over both implementation readiness and the effectiveness of the operating model once the new requirements become effective. Potential areas of focus include:

Governance and oversight

- Governance and programme oversight for Basel 3.1, SDDT and operational resilience implementation, including accountability, delivery risk, interdependencies and readiness.
- Board and executive oversight of implementation risks, key decisions, regulatory readiness and the effectiveness of escalation and challenge.
- Governance and completeness of material third-party inventories, supporting data and oversight of key external dependencies.

Regulatory and incident reporting

- Effectiveness of end-to-end regulatory reporting processes, including governance, automation, data lineage and quality controls supporting Basel 3.1 reporting.
- Controls supporting regulatory reporting and public disclosures.
- Operational incident identification, classification, escalation and regulatory reporting processes, including the quality and timeliness of decision-making.

Capital, methodology and data

- Design and implementation of new capital calculation methodologies, including supporting controls, data quality and model governance.
- Adequacy of data governance, including the completeness, accuracy, traceability and availability of data supporting prudential calculations and reporting.

Strategic implementation decisions

- SDDT eligibility assessments and implementation decisions, where applicable.
- Strategic Basel 3.1 decisions, including capital optimisation, risk appetite, balance sheet implications and internal model strategy.

Operational resilience and continuous improvement

- Operational resilience governance, scenario testing, remediation and continuous improvement activities.
- The interaction between operational resilience, technology change, cyber risk and third-party dependencies, including whether risks arising across these areas are identified and managed on an end-to-end basis.

Internal Audit should also consider whether assurance plans appropriately reflect the interaction between prudential regulation, operational resilience, technology change, regulatory reporting, data governance, and third-party risk, rather than reviewing these topics in isolation.



T+1 accelerated settlement



From 11 October 2027, the UK, EU and Switzerland have committed to transition the standard settlement cycle for in-scope cash securities transactions from T+2 to T+1, aligning with global markets that have already made the move. This is more than a one-day reduction: it materially compresses the time available to resolve breaks, source cash or securities and complete manual interventions. The transition therefore changes the risk profile of post-trade activity and places a greater premium on timely, automated and resilient processing.



The European transition is particularly complex. It spans multiple jurisdictions, currencies, time zones, central securities depositories and market infrastructures, creating significantly greater coordination challenges than the North American transition (May 2024). The lessons from that move only travel so far, because Europe's fragmentation multiplies the number of parties each firm depends on to settle. Confidence in your own readiness therefore counts for little if the counterparties, custodians and infrastructures you rely on are not ready, leaving you exposed to weakness further along the execution-to-settlement chain.



The regulatory clock is now the binding constraint, with key readiness milestones arriving before go-live. In the UK, the AST Code expects trade-date allocation and confirmation processing and implementation of the FMSB SSI Standard by 31 December 2026. These are industry requirements, but the FCA has signalled that inadequate preparedness may attract supervisory intervention. In the EU, equivalent requirements are expected to apply from 7 December 2026 under the CSDR Settlement Discipline RTS and will be directly enforceable once effective. For firms active across both markets, the implication is the same: core trade-date processing needs to be operational before 2027 industry testing.



Progress across both jurisdictions remains uneven. In August 2026 the FCA reported that most firms it has engaged with are moving in line with expectations, while some remain considerably behind, with particular concern around parts of the buy-side community. Continued reliance on manual processes, fragmented data and legacy controls across post-trade operations compounds the challenge. ESMA's messaging points the same way, warning that insufficient preparedness creates operational and reputational risk and may make counterparties less willing to trade with firms that cannot settle on time. The FCA has warned that unprepared participants may face supervisory action, and that its own supervisory approach will become increasingly intrusive as the deadline approaches.



T+1 is more than a compliance deadline. Handled well, it is a catalyst to strengthen automation, straight-through processing and data quality, and to cut operational and counterparty risk. The UK, EU and Swiss authorities have reinforced this with a joint industry Testing and Readiness Plan, which urges firms to start testing early and across the full settlement chain. That is the crux: the pressing question is not only whether a firm is ready itself, but how well it understands, tests and manages the readiness of the market participants across its settlement chain.

T+1 accelerated settlement (continued)

Key considerations for firms

Senior sponsorship, governance and strategic positioning

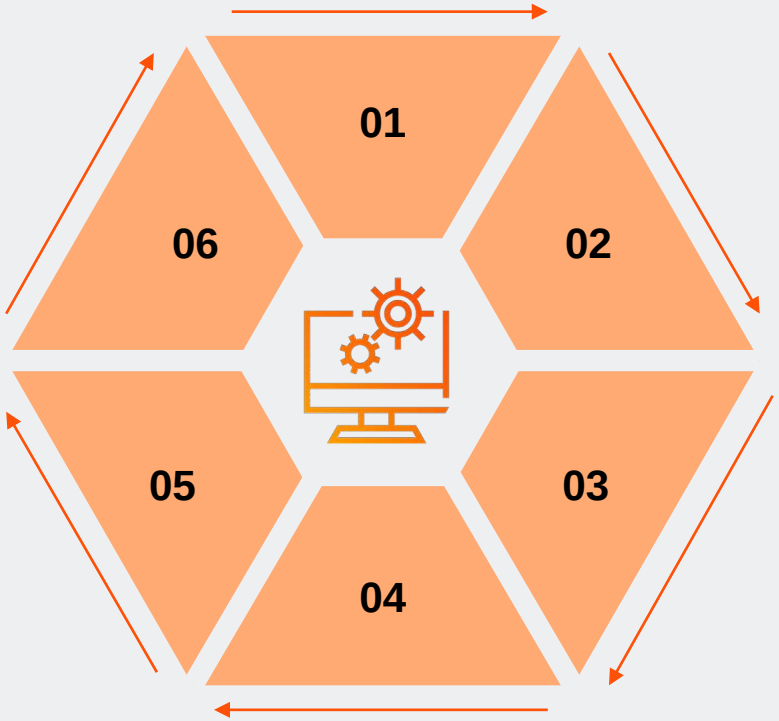
Treat T+1 as an enterprise-wide risk, change and franchise issue, not solely an Operations initiative. Clear executive ownership should bring together relevant business, Operations, Technology, Treasury / liquidity, Risk and client/service functions, with MI that allows senior management to challenge delivery, dependencies and residual risks. Beyond compliance, firms should consider how T+1 readiness affects client experience, service resilience and competitive positioning, and whether the investment being made creates a more automated, scalable operating model for faster settlement in future.

End-to-end and industry testing

Use 2026 to establish internal readiness so that 2027 industry testing proves the operating model rather than discovers fundamental gaps. Testing should cover the full execution-to-settlement chain, including counterparties, custodians, market infrastructures and critical providers, and reflect realistic volumes, exceptions, corporate events and stressed conditions. Firms should also demonstrate readiness for migration itself, including the first double-settlement day and failure of critical dependencies.

Trade-date processing, data quality and SSIs

Compress upstream activity sufficiently to support settlement on T+1. By the end of 2026, firms should be able to complete allocations and confirmations within applicable UK and EU timelines and implement relevant SSI market practices. Late allocations, SSI mismatches, weak PSET/static data and manual repairs become materially harder to resolve under T+1, increasing the importance of automation, accurate reference data and timely exception management.



Settlement performance and exception management

Understand current settlement performance and demonstrate that known weaknesses are being remediated before go-live. Firms should establish a clear baseline for fails, aged breaks and recurring exceptions, identify root causes and target areas of persistent underperformance. MI should distinguish structural weaknesses from isolated events and show where manual intervention or temporary workarounds remain necessary.

Funding, FX and liquidity

Assess how shorter settlement timelines change the timing and availability of cash, FX and securities inventory. Cross-border activity may create funding and FX mismatches, while greater use of T+0 repo and accelerated securities-lending recalls can increase intraday liquidity and inventory pressures. Firms should understand these exposures under normal and stressed conditions and make effective use of settlement optimisation, collateral and securities-finance tools where appropriate. The EU Gating Event is one such targeted tool for relevant T+0 repo and associated fixed-income activity, rather than a general solution across asset classes.

Clients, counterparties and third-party readiness

Treat external readiness as a core programme dependency rather than an assumption. Use allocation, matching and settlement data to identify clients and counterparties most likely to create bottlenecks, and obtain sufficient assurance over custodians, administrators, technology providers and other critical parties. Changes to cut-offs, data requirements and operating arrangements should be communicated early, with contingency plans for dependencies that remain materially behind.

T+1 accelerated settlement (continued)



Questions for leaders

01

Enterprise ownership and governance: Is T+1 being treated as an enterprise-wide risk, change and franchise issue rather than an Operations programme? Is there sufficiently senior sponsorship, clear accountability and effective governance across all materially impacted areas?

02

External dependencies: Where are we dependent on clients, counterparties, custodians, market infrastructure or critical providers whose readiness we cannot control? Do we know which dependencies could materially constrain our own readiness, and what our contingency is if they are not ready at go-live?

03

Migration and cutover readiness: Are we ready for the migration itself, including the first double-settlement day, production-volume processing and failure of a critical dependency? Are cutover governance, go/no-go criteria, contingency arrangements and accountable risk-acceptance decisions sufficiently clear?

04

Automation, data and manual dependency: Where do manual processes, poor data quality and legacy technology create the greatest risk under compressed settlement timelines? Are remediation and automation plans sufficiently prioritised, funded and on track to remove material dependencies before go-live?

05

Liquidity, FX and inventory: Do we understand the liquidity, funding, FX and securities-inventory implications of T+1 under stressed as well as normal conditions? Have intraday requirements, securities-finance dependencies and cross-market settlement-cycle mismatches been incorporated into planning?

06

Evidence of readiness: Can management demonstrate readiness through objective evidence rather than programme status alone? Are Boards receiving a clear view of settlement performance, testing outcomes, unresolved defects, temporary workarounds, third-party readiness and residual risk expected to be accepted at go-live?

T+1 accelerated settlement (continued)

Internal Audit considerations

Governance, challenge and risk transparency – assess whether governance drives timely decisions and if readiness reporting provides a transparent view of delivery, dependencies, unresolved issues and residual risk.

Scope, readiness and remediation – test whether all material T+1 impacts across products, markets, clients, systems and third parties have been identified, and whether remediation is complete, timely and appropriately evidenced.

End-to-end processing controls – assess whether controls across allocations, confirmations, matching, settlement, corporate events and exception management are designed for T+1 and can operate effectively under peak volumes, late activity and breaks.

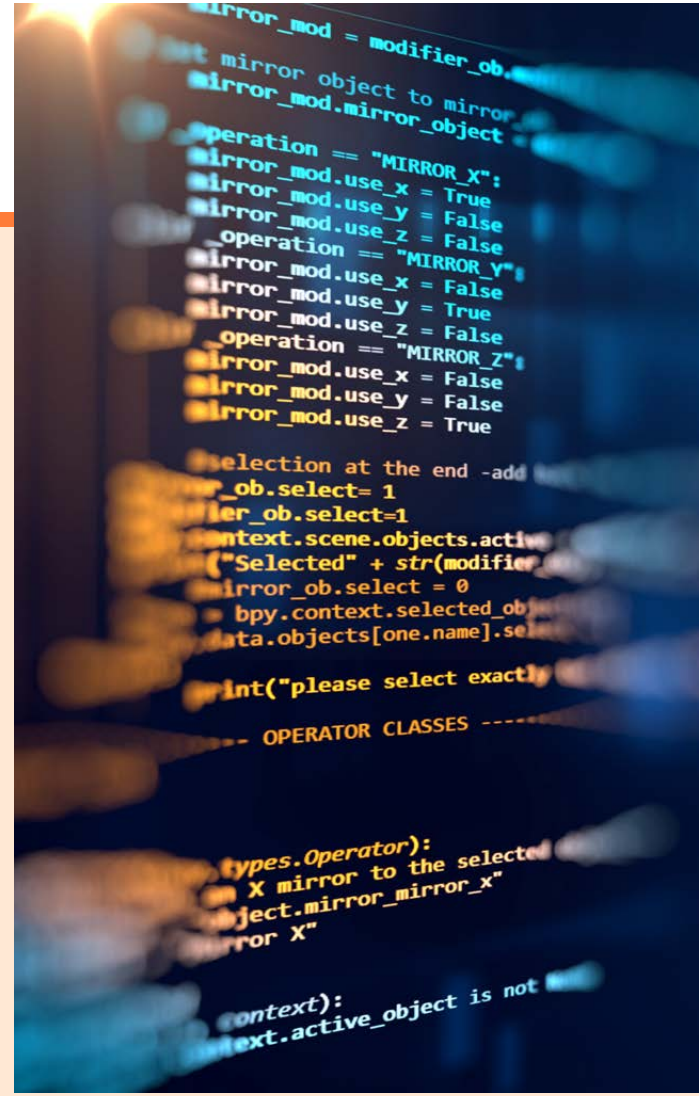
Data and settlement instruction effectiveness – assess whether weaknesses in SSIs, static and reference data create settlement risk, and whether issues can be identified and corrected quickly enough under T+1.

Funding, liquidity, FX and inventory resilience – test whether earlier cash, collateral, FX and securities requirements can be met under normal and stressed conditions, including intraday, cross-border and securities-finance pressures.

External dependency readiness – assess whether management understands where clients, counterparties, custodians, market infrastructure and critical providers could constrain readiness, and whether those risks are adequately mitigated.

Testing, cutover and contingency readiness – evaluate whether testing covers realistic volumes, exceptions, stress and third-party interactions, and whether cutover plans address the double-settlement day, critical dependency failure, go/no-go criteria and contingency arrangements.

Settlement performance and sustainability – test whether MI, thresholds and escalation enable timely identification of fails, aged breaks and recurring exceptions, and whether performance is sustainable without excessive manual intervention or temporary workarounds.



Risk landscape – Banking and capital markets



Financial and prudential risk

Capital adequacy and Basel 3.1, liquidity and funding, interest-rate risk, stress testing, recovery and resolution, regulatory reporting, RWA accuracy, Strong and Simple.

Credit and counterparty risk

Credit quality and concentrations, counterparty credit risk, NBFI exposures, leveraged finance, commercial real estate, private credit exposures, collateral and margin management.

Market and trading risk

Market risk, valuation controls, trading controls, transaction reporting, market abuse surveillance, conflicts of interest, algorithmic/electronic trading.

Operational resilience

Important business services, scenario testing, cyber resilience, crisis management, third-party concentration, cloud dependency, recovery capability.

Technology and data

Technology architecture, legacy technology, cloud, change and release management, data quality, regulatory data, AI/model-enabled processes.

Financial crime

Fraud, AML, sanctions, terrorist financing, proliferation financing, bribery and corruption, tax evasion, trade finance controls.

Customer and conduct

Consumer Duty outcomes, vulnerable customers, fair value, complaints and redress, access to cash/banking services, collections and forbearance.

Payments and digital finance

Payments modernisation, operational payments controls, stablecoins/digital money, digital assets, tokenisation, custody and settlement.

Wholesale market infrastructure

T+1 accelerated settlement, post-trade controls, clearing and margin, market infrastructure dependency, securities settlement, consolidated tape/market reform.

Model risk

Model inventory and governance, validation, model performance, stress-testing models, pricing/valuation models, AI/ML models.

Governance and risk management

Risk appetite, emerging-risk identification, SMF accountability, legal entity governance, risk aggregation, supervisory engagement.

Transformation and change

Regulatory change, finance/risk transformation, core-platform migration, cost transformation, integration programmes, operating-model change.

People and culture

Skills and capacity, conduct culture, remuneration and incentives, succession, non-financial misconduct, key-person risk.

Sustainability and climate

Climate financial risk, transition planning, financed emissions, sustainability disclosures, greenwashing, nature-related considerations.

Contact us and Glossary



Contact us

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



Nicole McManus

UK FS Internal Audit Leader

Partner

+44 (0) 7989 950485

nicole.r.mcmanus@pwc.com



Will Sankey

FS Internal Audit

Director

+44 (0) 7803 455666

william.t.sankey@pwc.com



Emily Farrer

FS Internal Audit

Senior Manager

+44 (0) 7483 419251

emily.farrer@pwc.com



Chris Jeffrey

FS Internal Audit Technology

Senior Manager

+44 (0) 7483 420563

christopher.jeffrey@pwc.com

Glossary of acronyms and abbreviations

AI/ML/DL	Artificial Intelligence/Machine Learning/Deep Learning
AIFM	Alternative Investment Fund Manager
AIFMD	Alternative Investment Fund Managers Directive
AML	Anti-Money Laundering
API	Application Programming Interface
BCM	Business Continuity Management
BoE	Bank of England
CASS	Client Asset Sourcebook
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIF	Critical or Important Functions
CSDR	Central Securities Depositories Regulation
CTP	Critical Third-Party
DORA	Digital Operational Resilience Act
ESMA	European Securities and Markets Authority
EU	European Union
FCA	Financial Conduct Authority
FRC	Financial Reporting Council
FS	Financial Services
FSB	Financial Stability Board
GDP	Gross Domestic Product
HM	His Majesty
HMT	His Majesty's Treasury
HVAC	Heating, Ventilation and Air-conditioning
IBS	Important Business Services
ICARA	Internal Capital Adequacy and Risk Assessment
IFPR	Investment Firms Prudential Regime
IFRS	International Financial Reporting Standards

Glossary of acronyms and abbreviations (continued)

IMF	International Monetary Fund
IPO	Initial Public Offering
IoT	Internet of Things
IT	Information Technology
KYC	Know Your Client
MI	Management Information
MiFID	Markets in Financial Instruments Directive
MPS	Model Portfolio Service
MTP	Material Third Party
MVC	Minimum Viable Company
NAV	Net Asset Value
NBFI	Non-Bank Financial Institution
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology, United States

OT	Operational Technology
OTC	Over-the-counter
PE	Private Equity
PRA	Prudential Regulation Authority
PQC	Post-Quantum Cryptography
RWA	Risk-Weighted Assets
SDDT	Small Domestic Deposit Taker
SDR	Sustainability Disclosure Requirements
SMCR	Senior Managers and Certification Regime
SMF	Senior Management Function
SWES	System-wide Exploratory Scenario
TCF	Treating Customers Fairly
TPRM	Third-Party Risk Management
UK	United Kingdom

Glossary of acronyms and abbreviations (continued)

UN	United Nations
US	United States
VFM	Value for Money
VPN	Virtual Private Network
WEF	World Economic Forum

Thank you

PricewaterhouseCoopers LLP is a limited liability partnership registered in England with registered number OC303525. The registered office of PricewaterhouseCoopers LLP is 1 Embankment Place, London WC2N 6RH. PricewaterhouseCoopers LLP is authorised and regulated by the Financial Conduct Authority for designated investment business and the Solicitors Regulation Authority for the provision of regulated legal services.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2026 PricewaterhouseCoopers LLP. All rights reserved. ‘PwC’ refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

pwc.com