Grant Thornton

Internal audit hot topics

Financial services

Spring 2026

Contents

Assurance as a key driver of growth

The financial services sector continues to balance shifting regulatory priorities with broader emerging risks such as ongoing geopolitical tensions, macroeconomic uncertainty and rapid technology changes.

As the regulators continue to streamline financial rules, internal audit is under increased pressure to do more with less and implement effective control frameworks that turn compliance into a strategic advantage. Firms that can effectively identify emerging risks and implement control frameworks are well placed to identify new opportunities for innovation. They're also best placed to promote structured and controlled growth in an operationally resilient and customer-centric environment.

Our quarterly financial services internal audit hot topics document is here to help you stay on track to refine your control framework and support your strategic growth plans.

Cross sector priorities

Macroeconomics and geopolitics

Ongoing geopolitical events and tensions continue to affect the economic landscape. Rising oil and gas prices may contribute to inflation and dampen economic growth, with a significant impact on businesses and consumers alike. If the current situation pushes up inflation and slows down growth, the Bank of England will need to make a decision in the round about interest rates. UK businesses will need to consider the impact on its people, strategy, international trade and key service lines (particularly for overseas operations).

Business continuity and resilience is a key consideration, and those in the financial sector will need to consider operational resilience practices to restore critical services in the event of an outage and reduce the potential for economic harm. The heightened geopolitical environment also increases the potential for state-sponsored cyber-attacks, and firms should ensure their cyber security controls form part of their wider resilience planning. Organisations will also need to consider how they manage evolving sanctions lists, with appropriate oversight and governance in place.

What should internal audit do now?

Internal audit should maintain a close view of the geopolitical and macroeconomic landscape, with the following activities:

- stress test and reverse stress test potential scenarios to identify situations with the most impact for the business, its people and its customers
- review current business continuity processes, supply chains and key third-party providers to mitigate the risk of service outages
- review financial crime controls, particularly around sanctions monitoring
- review cyber security processes, including critical services, to mitigate risks of state-sponsored cyber-attacks.

Financial crime

UK organisations continue to embed robust financial crime controls to meet emerging risks and align with regulatory expectations. This is particularly important given the heightened geopolitical environment and associated macroeconomic pressures. Key considerations are outlined below.

Economic Crime and Corporate Transparency Act (ECCTA)

ECCTA's 'failure to prevent fraud' offence makes organisations criminally liable if employees, subsidiaries, agents, or an associated person, commit fraud to benefit the organisation or its clients. Firms must be able to demonstrate that they have taken reasonable steps to prevent this, based on the six key principles of top-level commitment, risk assessment, proportionate risk-based prevention, due diligence, good communication, and effective monitoring. The offence has extraterritorial reach, and the penalty on criminal prosecution may be an unlimited fine.

While the new rules came into force in September 2025, organisations continue to fine tune their approach. Rather than duplicating existing fraud prevention activity, the focus should be on identifying gaps where current controls do not sufficiently address this offence. Key challenges include consistent and accurate reporting across multiple agencies; effective oversight over a broader range of individuals and organisations; and embedding an appropriate risk culture.

Managing sanctions

The Government's also updated its approach to enforcing sanctions, with several key publications in 2026. This includes the UK Government Strategic Approach to sanctions enforcement with up-to-date guidance on all government departments involved (covering both civil and criminal responsibilities), with breach examples, breach reporting practices and potential actions that could be taken.

Alongside this, OFSI published its strategy for 2026 to 2029 and its Financial sanctions enforcement and monetary penalties guidance. The strategy document describes the promote, enable, respond and change (PERC) approach to its operating model and KPIs to monitor their performance against the strategy objectives. These include faster and visible response to breaches using the full range of powers to deter and disrupt non-compliance and circumvention.

The guidance document provides details of new discounts on breach penalties that can be obtained for qualifying sanctions breach cases, such as:

- The Early Account Scheme, which affords up to 20% discount on the penalty subject to rapid, full breach disclosure with supporting materials and evidence for investigation.
- The Time Limited Settlement Scheme, affording up to 20% discount for a negotiated settlement (within a set timeframe and firms must waive the option of appeal or ministerial review).
- The Voluntary Disclosure Scheme with a discount of up to 30% for self-disclosure and ongoing co-operation.

To encourage uptake of these options, OFSI has increased the statutory maximum penalty to £2m and 100% of the value of the breach.

On identifying a breach, organisations wishing to make use of the new discount options will need to conduct an investigation and submit a prompt, clear and comprehensive report to OFSI. To be prepared, organisations should develop a planned response for breach investigations which includes mobilisation of external support to quickly ramp up investigation teams and make best use of the available time.

Money laundering controls for cash deposits

For financial services firms, the FCA recently published its FCA's regulatory priorities publication confirming that it'll continue to review money laundering controls around cash deposits. Key considerations include tighter limits over cash deposits, stronger verification and monitoring processes, appropriate staff training, enhanced Suspicious Activity Reports (SARs), mule detection, and greater use of the National Fraud Database.

Cryptoassets

Cryptoasset firms are moving within the FCA's regulatory perimeter, which carries a range of financial crime expectations. This includes applying a full anti-money laundering and counter-terrorist financing framework, with appropriate due diligence, know your customer processes and sanctions monitoring. In future, firms will also need to adopt the Senior Managers and Certification Regime (SM&CR) which includes prevention of financial crime as a prescribed responsibility and a dedicated Money Laundering Reporting Officer (SMF17); and adopt appropriate controls to safeguard funds and custody assets, in addition to financial crime reporting frameworks.

In addition to the above, the FCA is proposing a targeted Market Abuse Regime for Cryptoassets (MARC) to include disclosure of insider information, maintaining insider lists, clarifying legitimate market practices, information sharing, and embedding effective systems and controls.

What should internal audit do now?

Regardless of the sector, internal audit teams need to continue to improve their company's financial crime controls, ensuring they stay up to date with new and emerging risks. Key considerations include:

- Ensuring sanctions lists are updated, with effective breach investigation and response plans in place to mitigate further risks and make use of any available discounts.
- Identifying and addressing any gaps in the control framework against ECCTA's failure to prevent fraud offence.
- Reviewing wider governance and oversight processes to support ECCTA compliance, including reporting, training and risk culture.

Crypto firms will need to establish a robust financial crime framework, to meet the FCA's requirements for all firms and align with sector specific expectations on MARC. Internal audit will need to monitor these final developments and begin to embed the core principles as they move towards authorisation.

For the financial services sector, internal audit teams will need to closely monitor the FCA's review finding on cash-based money laundering. This includes effective horizon scanning, delivering targeted training programmes, and reviewing current verification and monitoring programmes.

Technology risks

Technology risk continues to feature prominently on internal audit agendas, with increasing interdependencies between cyber resilience, third-party risk, data governance and artificial intelligence (AI) adoption.

Alongside this, organisations are seeing a shift in their risk profile due to heightened geopolitical tensions and greater potential for state-sponsored cyber-attacks. With this in mind, key considerations for internal audit include:

- Whether their firm's cyber security processes are sufficiently robust, with a particular focus on ransomware and the growth of AI-enabled cyber attacks
- Incident response processes to maintain business operations and resume services promptly following a cyber incident or technology outage – which may be due to a cyber-attack, loss of a third-party service, a transformation programme (financial services firms also need to consider implications for Operational Resilience and Consumer Duty).
- The appropriateness of their firm's third-party risk management to ensure robust cyber security and ongoing services along the critical supply chain.
- The growth of AI, bringing new challenges on transparency, governance and ethics, in addition to use in sophisticated cyber-attacks, phishing and spreading disinformation.

What should internal audit do now?

Internal audit needs to monitor, assess and track technology risks in a joined-up way, rather than as separate workstreams. This includes reviewing resilience and recovery capabilities for critical business services, strengthening oversight of third-party providers and concentration risk.

As businesses continue to adopt AI, it's essential to ensure the activity is fair, transparent, explainable and repeatable – which is particularly important when supporting decision-making processes. Financial services firms must also ensure that client facing AI (for example to support credit scoring or chat bot services) operates within SM&CR conduct rules, and supports good customer outcomes. The PRA's model risk management principles cover AI/ML models, requiring strong validation and oversight of algorithmic decision systems. Where internal audit has previously considered the governance and oversight of AI within their firms, they are now starting to shift their focus and review the actual AI models and algorithms themselves.

Read more

Technology risk trends: Your key priorities for 2026

AI and data risks

AI and data risk are becoming increasingly prominent on internal audit agendas, as organisations move beyond traditional analytics into generative and agentic AI. These technologies introduce new interdependencies between data, models, decision-making and business processes, alongside heightened regulatory, ethical and reputational considerations.

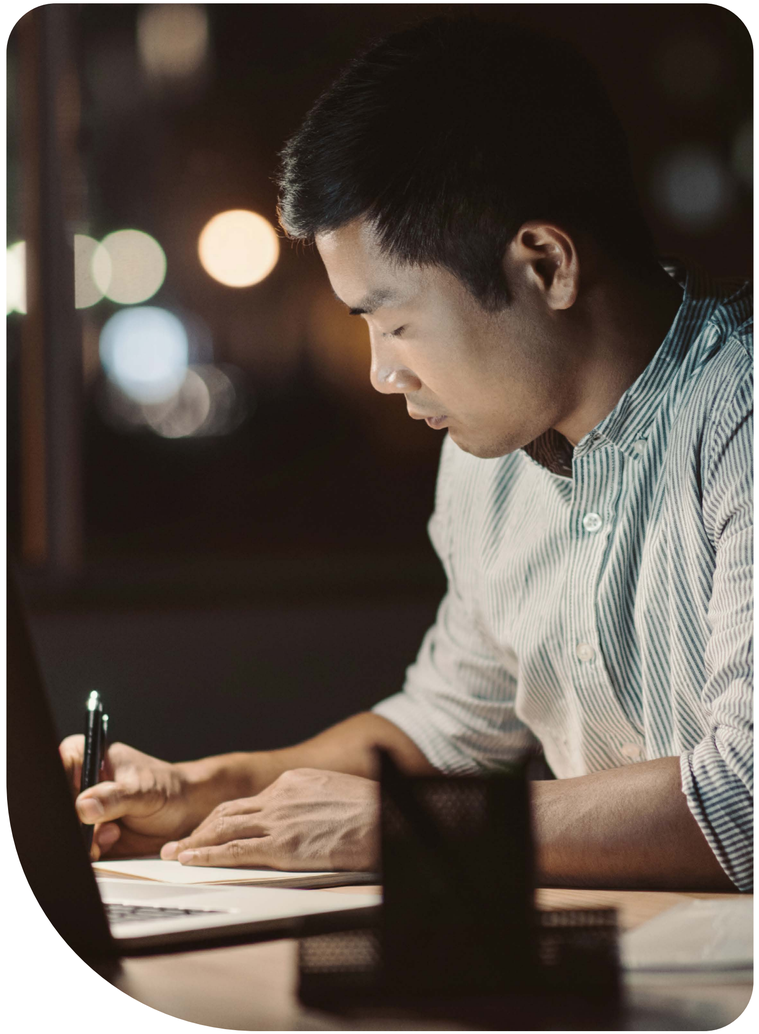
In addition to existing technology risks, organisations are seeing a shift in their risk profile due to the rapid adoption of AI tools across the enterprise that are often ahead of formal governance frameworks. In addition to governance of AI usage, internal audit needs to consider whether the organisation's data management practices are robust enough to support AI models, and the risks associated with agentic AI and autonomous decision-making.

Internal audit should also think about third-party risk management in relation to AI providers. This includes the organisation's approach to transparency and accountability for AI-driven decisions, and ethical AI use where technically compliant outcomes could nonetheless lead to customer detriment or regulatory scrutiny.

What should internal audit do now?

Internal audit needs to expand its approach to technology risk to explicitly incorporate AI and data risks as a distinct and evolving domain, rather than treating them as an extension of cyber or IT risk. To do this, firms must assess how the organisation uses AI in practice, moving beyond policy review to evaluate real-world behaviours including shadow AI usage. Internal audit may want to evaluate end-to-end AI lifecycle controls (from data sourcing and model development, through to deployment, monitoring and decommissioning); and review governance and accountability arrangements for AI-driven decisions and outcomes.

For higher-risk or autonomous use cases, it is important to assess whether appropriate human oversight controls are in place. Data controls specific to AI use (including quality, lineage, bias and fairness risks) should also be reviewed, along with third-party AI dependencies where organisations rely on external models or platforms. Supporting the development of AI assurance frameworks aligned to emerging standards such as ISO 42001 will help ensure a consistent and repeatable approach as adoption scales.



Corporate governance code – Provision 29

The revised UK Corporate Governance Code introduces more explicit expectations around boards' oversight of risk management and internal control frameworks. Under Provision 29, boards of UK premium listed companies must undertake an annual assessment of their material controls and provide a declaration on their effectiveness, for inclusion in the annual report.

The updated requirements place greater emphasis on how these controls are identified, documented, tested and evidenced. This will be familiar to organisations subject to US SOX, specifically for financial reporting, but Provision 29 is broader and extends across operational, compliance and reporting controls, including ESG. In practice, firms must refine their control inventories, clarify ownership and ensure robust evidence to support board-level conclusions.

- The focus has shifted from interpreting Provision 29 to embedding governance that can genuinely support a board declaration for 2026 reporting. Many businesses still have ground to cover. In our recent Corporate Governance Review, we found that in 2025, 45% of companies only partially met the Provision 29 requirements in their annual reports. Boards that treat Provision 29 as a live test of governance and accountability, rather than a future reporting exercise, will be better placed to meet the requirement.

What should internal audit do now?

Internal audit should ensure that boards and senior management have appropriate oversight over material controls, including clear criteria, definitions and monitoring processes. Key considerations include:

- Ensuring there's clear board ownership of material control definition and how effectiveness is reviewed and challenged.
- Defining material controls and prioritising risk focus.
- Monitoring how current risks align to agreed risk appetite.
- Defining an assurance approach to enable a conclusion on effectiveness that satisfies the board, mapping assurance activity across all three lines of defence.
- Prompt and demonstrable action over high-risk issues tied to material controls.

Internal audit teams are well-placed to assess whether governance over material controls is sufficiently robust, whether ownership is clearly defined and whether reporting supports effective board oversight and challenge ahead of required disclosures.

ESG

Regulatory expectations relating to ESG and climate risk continue to develop, with a growing emphasis on integration into core risk management and reporting frameworks. This includes a move to the UK Sustainability Reporting Standards (UK SRS), and under current proposals, UK listed companies will move from mandatory Taskforce for Climate-related Financial Disclosures to the new UK SRS Standard 2 (S2) from 2027. While based on the TCFD framework, UK SRS S2 is more prescriptive and includes more granular and specific requirements on strategy, governance, risk management and metrics. From 2029, companies will also need to report against UK SRS S1 on a comply or explain basis, covering broader sustainability-related risks and opportunities.

For financial services firms, the PRA has updated its expectations on managing climate-related financial risks with SS5/25, reinforcing the need to treat climate risk as a financial risk that should be embedded within existing governance and risk processes, including heightened expectations for Board involvement and the use of scenario analysis in strategic decision-making.

Firms must demonstrate how they reflect climate drivers in their strategy, risk appetite, scenario analysis and reporting, with effective governance and oversight in place.

What should internal audit do now?

Internal audit teams at financial services firms should conduct a gap analysis to ensure their existing climate risk management framework continues to align with evolving regulatory expectations as set out by the PRA. This includes reviewing governance structures, management information and use of data in internal decision-making and external disclosures. Any remedial action plans should be agreed by firms by 3 June 2026.

At listed organisations, internal audit teams can start by carrying out a UK SRS readiness assessment, followed by a gap analysis against UK SRS S1 and S2. This includes evaluating data quality, controls and reporting processes and developing an implementation roadmap.

Read more

FCA consults on UK Sustainability Reporting Standards

Alignment with the GIAS

The Institute of Internal Auditors' Global Internal Audit Standards (GIAS) took effect in January 2025, aiming to maintain quality and consistency across the sector through 15 principles covering five new domains. Internal audit is now expected to clearly articulate its strategy and demonstrate alignment with the organisation's wider business goals, reinforcing the function's burgeoning prominence as a strategic, value-adding partner.

A year on from the implementation date, the focus is shifting towards how well those changes have been put into practice. Embedding heightened governance requirements under Domain III remains particularly challenging. While it aims to foster greater collaboration between the Board and the internal audit function, it will take time to develop those relationships and build the necessary governance structures.

Crucially, the GIAS have also introduced mandatory topical requirements, giving subject-specific baselines to assess high risk or emerging topics (if in scope). While this improves standardisation, many internal audit functions will need to tailor their approach and draw on subject specific expertise to achieve sufficient depth.

There are four topical requirements published to date, covering cybersecurity (already live), third party risk (effective 15 September 2026), organisational behaviour (effective 15 December 2026) and organisational resilience (effective 15 December 2026). Of these, organisational behaviour is proving the most tricky to implement, given the challenges around the tangibility and measurement of culture.

At the time of writing, there are two additional consultations pending, covering anti corruption (due June 2026) and talent management (due October 2026). Organisations should monitor these publications and take the opportunity to help shape future standards.

What should internal audit do now?

Internal audit needs to demonstrate that it has moved beyond implementation into a mature operating model that aligns to the GIAS. Key considerations include:

- demonstrating how policies, procedures or strategy documents are applied in practice
- reviewing how the board and senior management continue to work with internal audit for maximum effectiveness
- ensuring appropriate skills sets are in place for topical requirements, and topic exclusion from the audit plan can be justified
- assessing whether internal audit strategy is clearly aligned to organisational objectives and risk priorities.

Operational incident and third-party reporting

In March 2026, UK regulators finalised a new framework governing how firms report significant operational disruptions and manage oversight of critical third-party relationships. The package was published jointly by the FCA, PRA and Bank of England through FCA PS26/2 and PRA PS7/26, alongside two pieces of finalised guidance (FG26/3 & FG26/4) setting out how firms should interpret and apply the requirements in practice. In-scope firms should assess their current operational resilience frameworks to ensure their regulatory reporting processes, formats and timelines continue to align with regulatory expectation.

Covering two separate regimes, operational incident reporting applies to almost all FCA-regulated firms, which are required to report as soon as reasonably practicable and within 24 hours of determining that an incident meets one or more of the FCA's thresholds (relating to consumer harm, safety and soundness, and market stability). Firms must document how they assess incidents against these thresholds to reach reportability decisions.

A two-tier approach distinguishes between standard reporting firms and enhanced reporting firms (including banks, enhanced scope SM&CR firms and non-bank payment service providers), which must provide more detailed updates and a final report within 30 working days. This means incident management, record keeping and management information will need to be maintained through to closure of the incident. Material third-party reporting applies to a narrower subset of enhanced scope firms and requires notification of new material third-party arrangements and submission of a register. The accuracy of third-party inventories and the consistent application of materiality criteria will be central to meeting these requirements. Dual-regulated firms must familiarise themselves with both the FCA and PRA regimes, which are largely aligned but retain regulator-specific thresholds. A single event may therefore give rise to different reporting outcomes or timelines depending on the regulator concerned.

What should internal audit do now?

With the new regime applying from March 2027, firms need to determine whether they are in scope of the incident reporting regime, the third-party reporting regime, or both. This assessment is likely to inform regulatory planning and Audit Committee discussions during 2026.

Priority actions include:

- reviewing incident classification and escalation processes against the new thresholds (including how responsibility for reportability assessments is assigned and how decisions are recorded)
- confirming whether the firm is subject to enhanced reporting obligations
- mapping existing third-party arrangements against the materiality criteria.

This may identify differences between internal third-party classifications and those expected for regulatory reporting purposes, including situations where a change in the materiality status of a third party would trigger a reporting obligation.

Firms already subject to comparable requirements, such as DORA or PRA SS2/21, should assess alignment and identify any gaps. Some firms may also consider a focused review of reporting readiness ahead of March 2027, covering governance, data and controls.

Banking and capital markets

Crypto authorisation

Cryptoasset firms are moving within the FCA's perimeter from October 2027. As such, crypto firms serving UK customers will need authorisation to continue regulated activities. These activities include (but aren't limited to) operating a qualifying cryptoassets trading platform, or dealing in qualifying cryptoassets as a principal or agent.

The authorisation window runs from 26 September 2026-28 February 2027, and firms will need to meet key criteria covering: threshold conditions; principles for business; governance and systems requirements; senior managers and certification regime; and conduct of business. Firms should be prepared for FCA regulation at the point of application.

Any existing approvals under payment services, e-money, or money laundering regulations won't convert automatically and firms will need to obtain a variation of permissions or apply for full authorisation. The same applies to firms currently using an s.21 approver for financial promotions.

What should internal audit do now?

Internal audit for firms undertaking crypto activities for UK customers need to carry out a gap analysis to identify which, if any, of their activities will be regulated. From there, a readiness assessment will help establish next steps for full authorisation and firms may need to update their current legal, governance and management structures to meet FCA expectations. Effective preparation is essential as the FCA doesn't typically allow for significant changes throughout the application process. As such, firms can benefit from the FCA's dedicated information sessions and pre-application support service (PASS).

Read more

Crypto firms – a guide to FCA authorisation

Non-financial misconduct

The FCA has published PS25/23 finalising its updated guidance for tackling non-financial misconduct. This framework previously applied to banks, but the FCA is now extending it to all Senior Management and Certification Regime firms (SM&CR) from 1 September 2026. The framework recognises that behaviours such as violence, bullying or harassment between colleagues are more than HR issues. They represent a material risk to the business.

The updates include changes to the Code of Conduct (COCON), and the fit and proper test for employees and senior personnel sourcebook (FIT), with fresh guidance for good practice application. Under the new rules, firms may take into account proven or unproven allegations relating to an individual's private life and social media activity when assessing fitness and propriety, but only where such conduct indicates a material risk to fitness and propriety. Firms are not expected to investigate trivial, implausible or speculative allegations. Social media activity can be relevant but must be considered in its proper context, holding controversial views, in itself, does not amount to misconduct.

Given the overlap with HR, firms will need to consider how the rules interact with key elements of employment law coming into effect across 2026, namely the duty on employers to take all reasonable steps to prevent harassment, adding sexual harassment to whistleblowing categories, and new rules that void clauses preventing employees from talking about discrimination or harassment, or an employer's response.

Non-financial misconduct

The new rules will affect financial sectors differently and it's essential for firms to identify where they could face the biggest exposures, as noted below:

- Investment banking – key considerations include interpersonal conduct, with additional training and focused work to establish and maintain the desired culture.
- Retail banking – the scope may include behaviour of customer facing staff at social or community events that are backed by the firm.
- Wholesale and retail insurance – the rules could apply to interactions with other market participants or industry events; brokers and underwriters need a standardised approach to apply across all aspects of the market, and London market firms' frameworks must be interoperable with Lloyd's expectations and byelaws.
- Asset and wealth management – smaller firms need to formalise informal culture processes, and portfolio managers or analysts may need to consider any behaviours that affect decision making or team dynamics.

What should internal audit do now?

To address the above, firms need to assess which activities and environments are in scope of the framework, and carry out a gap analysis. From there, HR and risk management teams need to work together to ensure all employees receive additional training, with senior leadership establishing the tone of the top in terms of culture. Firms also need effective processes to co-ordinate information flows and ensure crucial information is taken into account when carrying out fitness and propriety assessments.

Read more

Non-financial misconduct – embedding the rules

Basel 3.1 and SDDT

The PRA has published final rules in January 2026 for Basel 3.1 and Small Domestic Deposit Takers (SDDT) regime, with minimal changes from the proposals and near final rules published in September 2024. Most elements of the frameworks take effect on 1 January 2027, and firms can now move forward with greater confidence over their implementation plans.

Key changes in the final Basel 3.1 rules include minor updates and clarifications covering own-funds requirements, credit risk management, market risk, capitalisation of foreign exchange permissions, and disclosure and reporting templates (among others). The regulator has also confirmed that the interim capital regime won't be going ahead as the dates for SDDT and Basel 3.1 are now aligned.

The PRA hasn't made significant changes to SDDT either, but there are a number of minor updates for clarity, including over reporting requirements.

What should internal audit do now?

Firms are already well under way with their Basel 3.1 and SDDT implementation plans. But with the implementation deadline looming, it's essential to stay on track and ensure the project draws on synergies with broader compliance frameworks. Next steps for internal audit teams include:

- Perform a review of the impact assessment and document how the new rules have been interpreted, including key assumptions, and expected changes to Pillar 1 and Pillar 2A capital requirements.
- Mapping and testing all models and systems to ensure they're working as expected, and are fully embedded across the business.
- Reviewing all reporting expectations and ensuring systems and processes are updated and fully tested.
- Ensuring adequate skilled resources are available to support implementation.
- Keeping the Board updated on implementation progress for Basel 3.1 and SDDT standards.

Read more

Basel 3.1 and SDDT regimes – PRA issues final rules

Buy now, pay later

The FCA has published its final rules on buy now, pay later (BNPL) lending, bringing these activities within the FCA's regulatory perimeter. Recognising the benefits that BNPL can offer, the FCA wants to support growth and innovation through proportionate regulation that reduces the risk of harm to consumers. Following on from consultation paper CP25/23, published in summer 2025, key changes to the final rules include:

- Moving some content from the key product information section to additional product information to avoid overwhelming consumers – including details on how to withdraw or cancel a product, or finish payments early.
- Clarifications and amendments to consumer communications following a missed payment – specifically noting that firms don't need to notify a guarantor (if applicable) following a missed payment, but lenders do need to make borrowers aware of the potential (non-exhaustive) negative consequences.
- Confirmation that BNPL activities will fall under the compulsory jurisdiction of the Financial Ombudsman Service, but not the voluntary jurisdiction.

For firms seeking authorisation for BNPL activities, the FCA registration window runs from 15 May 2026 to 1 July 2026 and the regulations apply from 15 July 2026 (with a six-month temporary permissions regime). Lenders can continue to support BNPL agreements before that date, but they can't issue any new ones without authorisation.

What should internal audit do now?

To get started, BNPL lenders need to assess current practices against new regulatory expectations, ensuring they meet FCA requirements across governance and oversight, risk management, data collection, reporting and Consumer Duty, among others. Many firms will need to focus on client communications and client understanding, ensuring they understand key information and the potential impact of the agreement.

Read more

BNPL regulation – FCA confirms the final rules

Targeted support

The FCA has published PS25/22, with the near-final rules for targeted support. The initiative aims to bridge the financial advice gap and help individuals achieve good customer outcomes through more personalised support for customers in particular scenarios that stops short of an individual recommendation. This can be particularly helpful in key areas such as investments, pensions, long-term savings and protection.

To deliver this, firms can group consumers with similar needs, circumstances or characteristics, and use pre-set courses of actions or a series of prompts to help them make more informed financial choices. Crucially, firms must not recommend a personalised course of action to individuals, and the risk of being perceived to have given financial advice will be the most challenging area for compliance.

Firms wanting to deliver targeted support must be approved by the FCA, and the gateway for registration is open now. Approved firms can offer targeted support from 6 April 2026.

What should internal audit do now?

First and foremost, firms need to decide whether to offer targeted support, weighing up the benefits to consumers, the commercial opportunities and the regulatory risks. Key actions for internal audit teams of firms considering offering targeted support include:

- Assessing the products or services where targeted support could apply.
- Identifying which customer segments could benefit from targeted support.
- Reviewing how potential courses of action can benefit these segments.
- Developing the necessary governance, controls, training and oversight frameworks.

Many firms will rely on digital tools and analytics to deliver targeted support. So, it's essential to ensure the underlying data and technology processes are robust, fully tested and fit for purpose.

Read more

FCA confirms targeted support framework

Article 21c – remote banking services

Under Article 21c of CRD VI, third country undertakings can't continue to offer core banking services remotely. Moving forward, non-EU banks will need to establish a branch in each EU country that they operate in, or a subsidiary with passporting rights. This has significant and fundamental implications for a bank's operating model and takes effect from 11 January 2027.

With a short implementation window remaining, most banks have determined which territories to continue operating in, and whether to establish branches or a subsidiary or, in most cases, make use of eligible exemptions. Firms are also in the process of making the necessary booking model changes, and transitioning client contracts to meet the new operational structure.

What should internal audit do now?

Banks need to ensure they have appropriate governance, oversight and compliance processes in place, which align to regulatory expectations. Key actions to take now include:

- Updating business models to reflect the new operating structure.
- Continuing with authorisation and licensing processes ensuring adequate financial and physical, resources throughout.
- Amend existing processes to avail of exemptions and meet reporting requirements.
- Ensure relevant teams have adequate training to support the use of exemptions and a smooth transition.

Read more

Authorising third-country branches under CRD VI

Private credit

High-profile market events have brought private credit under greater regulatory scrutiny. With diverse private credit structures and a broad range of market participants, firms need greater oversight over their exposures, with concerns around valuations, transparency and liquidity mismatches and redemption pressures. Where these activities form part of broader capital or funding strategies, regulators expect firms to manage these risks effectively, taking into account their systemic impacts.

As part of this wider focus, regulators are looking at how firms manage securitisation, synthetic risk transfers and significant risk transfers. The key issue is the extent to which these transactions achieve genuine and sustainable risk transfer, particularly where they have a material impact on capital positions. As such, regulators are keen to ensure greater transparency over these risks including effective counterparty risk management, robust model risk, and appropriate data quality for valuations.

What should internal audit do now?

Firms should review whether governance, risk appetite and reporting frameworks provide sufficient visibility over private credit and structured transactions. This includes reviewing underwriting standards, ensuring due diligence processes are applied consistently, and evaluating whether management information captures key exposures and risk concentrations.

For securitisation and SRT activity, firms should review current risk management processes to ensure they align with PRA expectations around commensurate risk transfer, including effective data aggregation and robust model risk processes.

Read more

Private credit – a public issue for insurance

Motor finance

Motor finance lenders continue to face uncertainty regarding the FCA's redress scheme. The final rules were published on 30 March 2026 (PS26/3), and were subsequently challenged by three lenders and one consumer group.

The FCA has since confirmed that it will defend the scheme, but the case is unlikely to be heard before October. In the meantime, the regulator asks firms to focus on key actions that would be needed across all scenarios. That includes identifying relevant complaints, gathering data, working with claims companies, and ensuring full co-operation with the Financial Ombudsman Service. Consumer communication timelines have also been relaxed, although the FCA will assess whether additional engagement is needed.

The legal challenge could result in a revised scheme, which would be subject to further consultation and potential further legal challenge. There's also the potential for no redress scheme, with a complaint-led scenario instead. The FCA urges firms to make contingency plans on that basis, noting the following:

- the complaints pause wouldn't be extended
- a tribunal decision could be made around mid-November, and firms should be ready to handle complaints from then (with usual statutory deadlines in place)
- the FCA won't immediately offer further guidance or rules after the tribunal, and firms will need to draw on legal findings
- the FCA expects firms to proactively contact customers who haven't complained.

What should internal audit do now?

While the direction of travel is still unclear, work on motor finance could move quickly following the tribunal decision. So, internal audit needs to ensure the business has considered no regrets actions and robust contingency plans to cover multiple scenarios. Key considerations include:

- data and population identification, cleansing and validation, including use of proxies where underlying data isn't available
- effective oversight, governance and MI, to support post-tribunal decision-making and readiness
- evidence that the relevant senior manager has taken reasonable steps to discharge their responsibilities throughout
- appropriate customer communication that's clear and easy to understand, in line with Consumer Duty expectations.

Through their governance forums, firms should also document their contingency plans for applying the existing redress scheme methodology, following a revised scheme or taking a complaint-led approach.

Read more

FCA motor finance redress scheme – a guide to the final rules

Recovery and resolution

The UK's largest firms are currently preparing for the PRA's third Resolvability Assessment Framework (RAF) cycle, with a focus on restructuring planning. Looking beyond the framework design, banks must test how their capabilities would work in practice not just on paper.

Earlier RAF cycles were largely concerned with establishing core capabilities, including valuation, liquidity, operational continuity and restructuring planning. The forthcoming cycle is expected to assess how these capabilities function together, particularly where firms need to execute multiple actions simultaneously and under time pressure, and the Bank of England will want to see evidence of remediation work over any outstanding issues from previous assessments. This includes work to strengthen data, improve the usability of management information, and ensure that plans are sufficiently detailed to support execution.

Alongside RAF preparations, the PRA published a package of resolution simplification measures in March 2026 covering:

- PS9/26 streamlines Minimum Requirement for Own Funds and Eligible Liabilities (MREL) reporting by deleting the MRL002 forecast template and refining data elements in MRL001 and MRL003, effective from 1 January 2027.
- PS10/26 raises the RAF reporting threshold from £50bn to £100bn in retail deposits and reduces the recovery plan review frequency for small domestic deposit takers to once every two years.
- PS11/26 introduces standardised MREL disclosure templates and requires firms to include a qualitative narrative on capital distribution constraints in their Pillar 3 disclosures.

While these updates reduce the reporting burden for firms, the PRA's expectations around operational readiness and governance standards remain unchanged.

What should internal audit do now?

Internal audit and second-line teams should assess whether existing assurance provides a realistic view of resolvability, and whether any remaining gaps could affect execution in practice. It's essential to demonstrate operational readiness, including testing whether key capabilities such as valuations, liquidity reporting and service mapping can be delivered accurately and at pace. Outputs should be assessed in the context of real decision-making requirements under stress scenarios.

Restructuring plans must be sufficiently detailed and actionable, with clear alignment to the firm's preferred resolution strategy. Firms should also ensure that governance and escalation processes are capable of supporting timely and effective decision-making in a stressed environment.

Mortgage priorities

The FCA published its 2026 Regulatory Priorities report for the mortgage sector in March 2026, covering three key areas. The first is improving consumer outcomes under the Mortgage Rule Review, where the FCA wants to enable a market that can adapt, innovate and meet consumer needs across different life stages. Firms are expected to engage with the review and its focused later life mortgage market study, with a policy statement anticipated in H2 2026.

The second priority is encouraging responsible lending and supporting borrowers in financial difficulty, with a focus on affordability assessments, appropriate forbearance, and second charge lenders. The FCA is clear that rebalancing risk involves trade-offs, but that responsible lending and high standards of conduct remain core principles. The third priority is ensuring the quality of advice, with firms expected to recommend products that are suitable for consumers' needs, including those consolidating debt or borrowing into later life, and to test outcomes across the customer journey.

What should internal audit do now?

Internal audit teams at mortgage lenders need to review how the firm is engaging with the Mortgage Rule Review, including how potential rule changes are being tracked and reflected in product and risk appetite frameworks. Firms need to ensure affordability assessments remain appropriate and well-evidenced, particularly where existing flexibilities have been applied to broaden access. Advice quality frameworks need to be reviewed against the FCA's updated expectations, with particular attention to outcomes monitoring and record keeping.

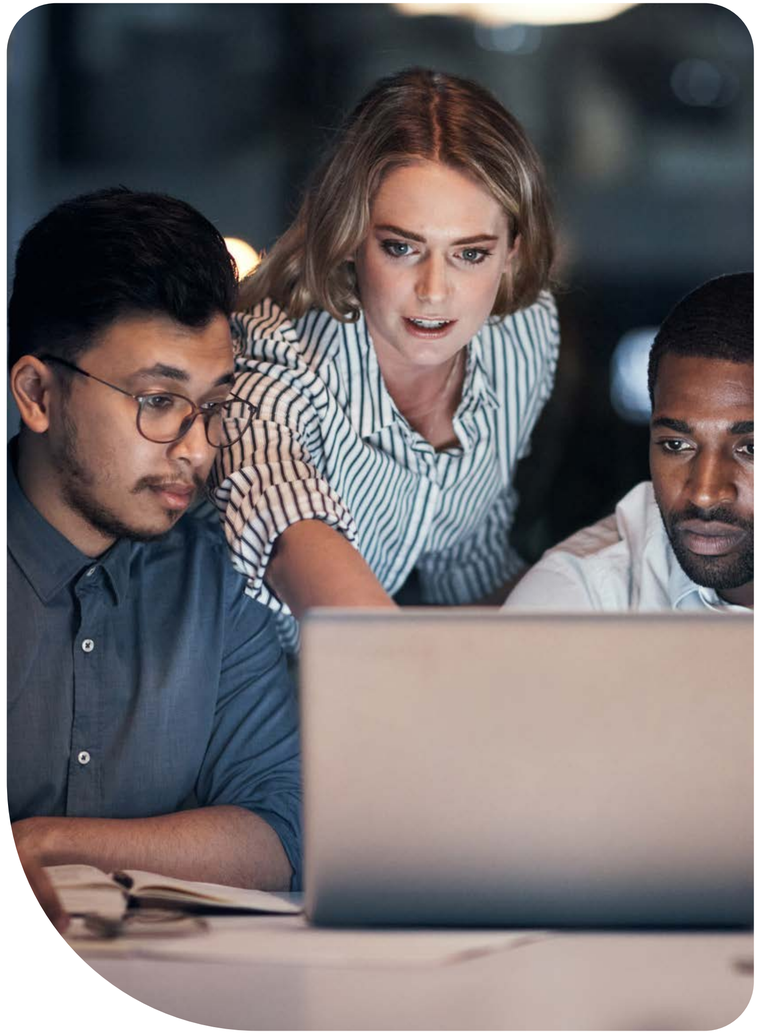
Liquidity framework modernisation

The PRA published CP5/26 in March 2026, setting out proposed enhancements to the UK liquidity framework. The consultation reflects supervisory observations from recent periods of market stress, which highlighted the pace at which liquidity demands can crystallise under certain conditions. Rather than increasing headline liquidity requirements, the proposals focus on improving firms' operational readiness and their ability to deploy liquid resources effectively in stress scenarios.

Key proposals include extending internal liquidity stress testing to cover rapid firm-specific outflows over a seven-day timeframe, in addition to existing monthly requirements. Firms would also need to remove the existing exemption that allows Level 1 assets, including sovereign bonds, to be excluded from annual monetisation testing. On central bank facilities, the PRA proposes that firms may recognise drawings from non-emergency facilities in their overall liquidity adequacy assessment, provided they can demonstrate operational readiness, including adequate pre-positioned collateral and tested access.

What should internal audit do now?

The consultation closes on 17 June 2026, and firms need to engage with the proposals and consider how they apply to their current liquidity risk management frameworks. Key areas for internal audit to consider include whether existing stress testing adequately captures short-timeframe scenarios, whether monetisation testing covers Level 1 assets, and whether governance and collateral arrangements would support access to central bank facilities in stress. Where gaps are identified, firms will need to factor these into their ILAAP and broader contingency planning ahead of the final rules being confirmed.



Asset management

Conflicts of interest and conduct oversight

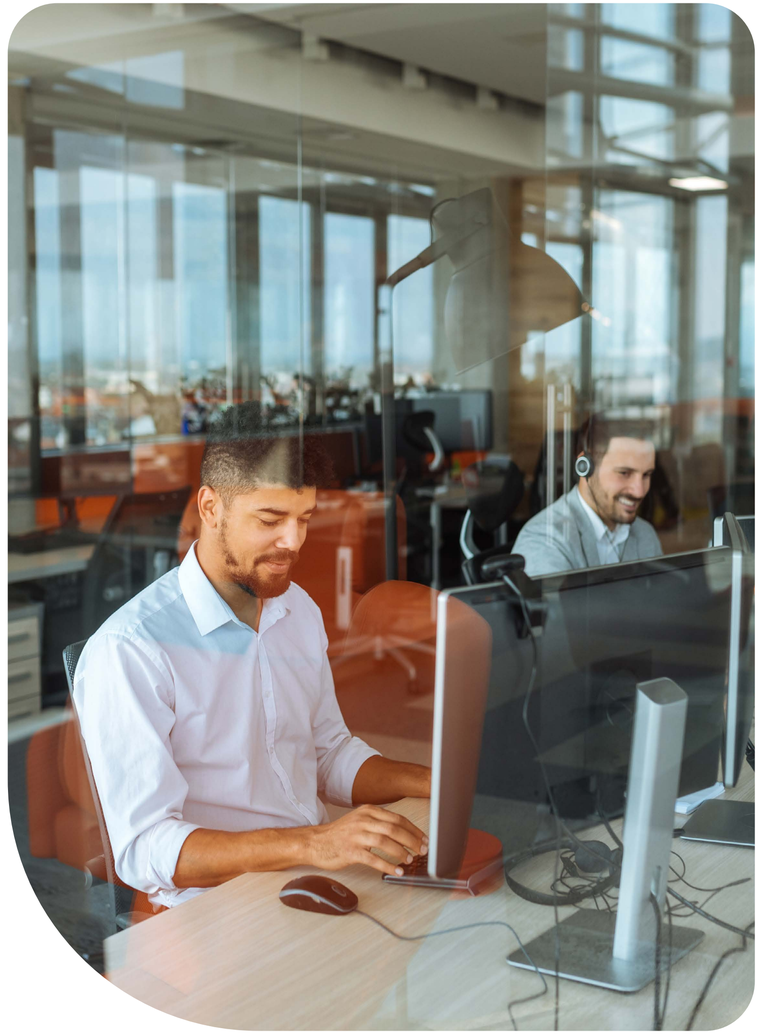
While the FCA acknowledges areas of good practice around conflict management, it highlights further work ahead to maintain trust in the market. If left unchecked, this could result in poor customer outcomes through mispricing, misuse of confidential information, or biased advice. Key weaknesses include evidencing conflict identification, management and escalation, and demonstrating that behaviours and decisions consistently support fair client outcomes.

To address these issues, the FCA's launching a broad supervisory programme targeting conflicts and poor conduct across firms' trading and originating activities in securities markets. It will also review wholesale conduct rules, conflicts management practices across trading and origination activities, and broader market structure and transparency reforms (including transaction reporting and conduct frameworks).

What should internal audit do now?

Internal audit needs to ensure robust processes to effectively identify and proactively manage conflicts of interest. This includes monitoring emerging risks as the business model, strategy or technologies evolve. Key considerations include:

- Review all related processes and procedures on how conflicts are identified, documented and addressed, and consider how well these are practically implemented.
- Assess governance arrangements, including senior oversight, MI and escalation processes.
- Map current practices with key areas of FCA focus to prepare for regulatory scrutiny and ensure alignment with industry-wide good practice.
- Test the consistency and effectiveness of conflicts training and awareness across all three lines of defence.



Adoption of new technology

Wholesale market firms continue to adopt new technologies such as AI, digital assets, distributed ledger technology and quantum computing. While the FCA is keen to support innovation, firms need to ensure they can adopt these tools in a way that aligns with operational resilience expectations and promotes good customer outcomes.

To achieve that, the FCA expects firms to actively engage with regulatory sandboxes and industry innovation initiatives, such as the Digital Securities Sandbox and AI Lab. Firms also need to embed robust governance and accountability processes, taking into account any third-party risks and relationships.

Alongside this, the FCA is finalising its cryptoassets regime and will continue to engage with firms to understand how new technologies are being applied across the sector.

What should internal audit do now?

The speed of innovation continues to increase, and internal audit needs to assess whether governance, accountability and controls are keeping pace. Key activities include:

- Review governance frameworks for emerging technologies to ensure clear oversight and accountability, and alignment with the broader risk appetite.
- Assess model development, testing, monitoring and change management arrangements, particularly where tools influence investment decisions or client outcomes.
- Evaluate third-party risk management for technology providers to maintain effective oversight, with key controls in place to mitigate data risks and concentration risk.
- Ensure effective processes to feed lessons from regulatory sandboxes or technology pilots back into the control framework.

Preventing financial crime and market abuse

Preventing financial crime and market abuse remain a key regulatory priority for the FCA. As such, the regulator expects wholesale markets and asset management firms to continue to strengthen their financial crime controls, monitor emerging risks and enhance surveillance. However, the FCA notes that firms should take a proportionate approach and is actively exploring ways of reducing the compliance burden for lower-risk activities to improve efficiency, including good use of technology.

Concerns over market abuse are partly driven by the FCA's Annual STOR for 2025, which found that insider dealing was the most prevalent form of suspicious activity, accounting for 82% of reports. In its supervisory work, the FCA also found that some market abuse surveillance processes were not tested or governed appropriately, and key issues included weak data feeds and poorly calibrated alerts.

In addition to ongoing financial crime work, the FCA will continue its STOR supervision programme throughout the year, and publish its final policy statement on improving the UK transaction reporting regime.

What should internal audit do now?

To continue to meet FCA expectations, internal audit should review the current financial crime and market abuse framework to ensure it is designed effectively and operates as intended. Key activities include:

- Assess whether surveillance coverage spans all relevant asset classes, trading strategies and communication channels.
- Review alert handling, escalation and STOR decision making processes, including governance and audit trails.
- Test the quality, completeness and lineage of data feeding surveillance systems.
- Ensure any use of AI or advanced analytics tools are appropriately monitored, and are explainable, repeatable and fair.

Insurance

Premium Finance and Pure Protection

The FCA's published the final findings from its Premium Finance market study, and its interim findings on Pure Protection. In both cases, the regulator has opted not to introduce sector-wide interventions, instead focusing on effective application of Consumer Duty – specifically, fair value assessments. Firms that can't justify their price in relation to customer benefits will face greater scrutiny moving forward.

Key findings in Premium Finance highlight that there's still significant variation in price and margin, although the FCA notes that market scrutiny has led to a drop in APR. However, the FCA found that fair value assessment methodology was sometimes incomplete or inadequate (including inconsistent documentation on target markets) and supported by limited underlying assumptions. Where firms did have clear fair value policies and processes, they weren't always consistently applied.

Regulatory messaging was similar for Pure Protection. Although the FCA believes the market is largely working effectively, there are areas for improvement, namely: poor practice from some intermediaries, application of customisable practices (which is fine in theory), commission for over-50s guaranteed cover and income protection claims ratios. There's also a protection gap and the FCA is looking at how to reduce barriers to entry to promote market growth, including through targeted support.

What should internal audit do now?

Insurance firms should review their premium finance and pure protection products, to ensure they meet the needs of the target market. Looking along the broader distribution chain, firms need to ensure that all prices and fees (including commission), represent genuine benefits to consumers and are commensurate with the service provided. Key actions to improve the quality of fair value assessments include:

- Clearly identifying the target market for each product or service, to include a differential outcomes assessment for each customer segment or product.
- Making decisive judgements over whether a product offers fair value, and taking prompt action to remedy it if not.
- Taking a holistic view of fair value, and assessing it within the context of all other consumer outcomes.
- Reviewing the metrics used to assess fair value and ensure they're robust and fit for purpose.
- Ensuring appropriate oversight, governance and control frameworks for continuous review and assessment of fair value.

Read more

Premium finance: a greater focus on fair value assessments

Read more

Pure protection interim report – a positive outlook

Solvent exit for insurers

Insurers must have a solvent exit plan in place by 30 June 2026, ensuring that these plans will work in practice and are more than a hypothetical exercise. However, this has proved more complex than many firms initially anticipated, and there's significant work ahead to meet the deadline. Key challenges include:

- Effective co-ordination across actuarial, finance, legal and operational teams, supported by strong governance, accountability and assurance.
- Difficulties in imagining severe, yet plausible, events that could trigger a solvent-exit.
- Financial models that have focused too heavily on capital metrics over liquidity during the exit period, and a need for more granular monthly cash-flow models.
- Considerations of inter-group and third-party dependencies

In addition to the above, many smaller firms have struggled with resourcing and balancing a range of competing priorities. Meanwhile, many larger firms have relied too heavily on their existing recovery and resolution frameworks and their Solvency II infrastructure, and have subsequently underestimated the scale of the project.

What should internal audit do now?

The PRA expects firms to obtain appropriate assurance over their solvent exit analysis, recognising that the quality of the analysis directly informs the effectiveness of the resulting solvent exit plan.

Some firms are seeking independent assurance from external providers, while others are using their own internal audit functions. Regardless of the approach, assurance teams must adapt their standard control testing methodology to ensure solvent exit plans are compliant with PRA expectations, rather than assessing key controls around the plan's application. This change in direction reflects the revised IIA code's repositioning of internal audit as a valuable consultant to the wider business.

Read more

Solvent exit planning for insurers – the final furlong

Claims handling

Last year's 'Which?' supercomplaint about home and travel insurance has brought claims management under closer regulatory scrutiny. While the FCA hasn't opted for a market study, it has identified claims handling (with a focus on consumer understanding and service quality) as a key regulatory priority for 2026. Effective application of Consumer Duty is paramount, to ensure customers understand their level of cover and receive prompt, clear and transparent support throughout the claims process.

The FCA will continue supervisory work with home and travel insurers, and review what actions they're taking to improve consumer understanding. Looking more broadly, the regulator will consider how it tracks claims, assess claims quality, review how varying sales processes affect consumer outcomes, and expand its oversight of outsourced claims processes.

What should internal audit do now?

Internal audit activity needs to consider whether the claims process supports good consumer outcomes, and what actions can be taken to support that earlier in the customer journey. Key considerations include reviewing:

- communications to improve customer understanding around coverage and claims processes
- claims decision timeliness, transparency and quality across all product lines
- governance and oversight of outsourced or delegated claims arrangements
- management information used to monitor Consumer Duty outcomes within the claims journey

Focused internal audit work can give senior stakeholders greater assurance that claims risks are understood, monitored and actively addressed to promote good consumer outcomes.

Bulk Purchase Annuities (BPA)

In its ‘Dear CEO’ insurance supervision letter from January, the PRA highlighted ongoing concerns about the bulk purchase annuities (BPA) market. High competition could weaken pricing discipline and negatively affect risk management standards, which combined with long-dated liabilities and high transaction volumes could lead to greater prudential risk.

Recognising the ongoing relationship between BPA and the funded re-insurance market, the PRA is putting the latter under greater scrutiny to ensure risks are appropriately managed. A recent Bank of England speech noted that the funded reinsurance market has grown quickly and could underestimate risk by not taking into account insurers’ increasingly complex investment landscape, including private credit risks and geopolitical factors. As such, the PRA has published CP8/26 proposing that new funded reinsurance transactions should increase capital held to 10% of liabilities (up from 2-4%).

What should internal audit do now?

As BPA volumes continue to grow, internal audit needs to ensure that governance and risk management frameworks are robust and adequately support long-term exposures. Key activities include:

- Reviewing pricing models, risk management and approval processes for BPA transactions.
- Assessing asset liability management arrangements, including reliance on illiquid and private credit assets.
- Evaluating liquidity stress testing and contingency planning under severe but plausible scenarios.
- Reviewing governance and oversight of funded reinsurance and associated counterparty risks.

This work can support prudent risk management, while continuing to strengthen policyholder protection.

Contact us

Rob Benson
Partner, Head of Financial Services
Business Risk Services
D +44 (0)20 7865 2415
E rob.m.benson@uk.gt.com

Ravi Joshi
Partner, Financial Services
Business Risk Services
D +44 (0)20 7865 2571
E ravi.joshi@uk.gt.com

Ryan Price
Partner, Financial Services
Business Risk Services
D +44 (0)20 7865 2578
E ryan.price@uk.gt.com

Chris Williams
Partner, Head of Large Corporates
Business Risk Services
D +44 (0)20 7865 2460
E chris.j.williams@uk.gt.com

Manav Soni
Partner, Financial Services
Business Risk Services
D +44 (0)20 7728 2940
E manav.soni@uk.gt.com

Shuvo Banerjee
Partner, Financial Services
Business Risk Services
D +44 (0)20 7865 2096
E shuvo.banerjee@uk.gt.com