Grant Thornton

Internal audit hot topics

Cross sector priorities

Spring 2026

Contents

Supporting innovation

Internal audit priorities continue to evolve amid rapid technology changes, ongoing geopolitical tensions and macroeconomic uncertainty.

As such, effective horizon scanning is essential to help internal auditors manage the operational implications of these emerging risks and opportunities, while maintaining a resilient business environment.

But effective internal audit is so much more than assurance. It's increasingly recognised as a valuable business partner that can help firms navigate emerging risks and identify new opportunities for innovation.

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

Key priorities for internal audit

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 their people, strategy, international trade and key service lines (particularly for overseas operations).

Business continuity and resilience is a key consideration, and organisations need to consider how they'll restore operations in the event of an outage. The heightened geopolitical environment also increases the potential for state-sponsored cyber-attacks, and organisations should ensure their cyber security controls form part of their wider resilience planning. It's also essential to consider how to 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. Businesses 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 need to 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 has 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.

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.

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.
- 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. Where internal audit teams have 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.

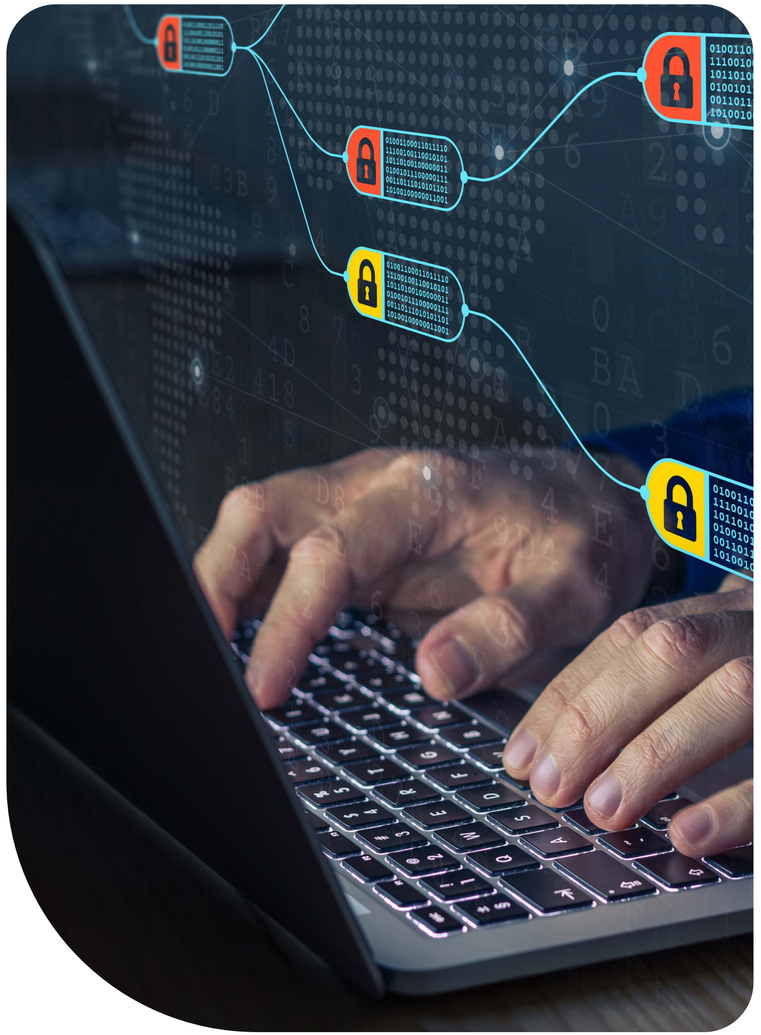
In addition to existing technology risks, organisations are seeing a shift in their risk profile due to the rapid adoption of AI tools across the enterprise that are often ahead of formal governance frameworks. In addition to governance of AI usage, internal audit needs to consider whether the organisation's 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.

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 is 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.

What should internal audit do now?

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 they have 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 skill 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.

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

Paul Rao
Partner, Business Risk Services
D +44 (0)16 1953 6303
E paul.rao@uk.gt.com

Ben Langford
Partner, Business Risk Services
D +44(0)20 7865 2437
E ben.langford@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

Emma Young
Partner, Business Risk Services
D +44 (0)20 7728 3496
E emma.young@uk.gt.com