



The Risk Agenda 2027

Commercial and Government

PwC

September 2026





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



Stephanie Edenborough

Partner,
Commercial and Government
Internal Audit Leader,
PwC UK

+44 (0) 7834 254859

stephanie.edenborough@pwc.com

Organisations will enter 2027 in an environment where disruption is more persistent, interconnected and difficult to contain. Geopolitical volatility is reshaping trade, supply chains and access to critical resources. Technology and Artificial Intelligence are changing operating models, workforce requirements and the pace of transformation. Cyber threats increasingly have operational and physical consequences, while reliance on complex supplier and technology ecosystems means disruption can travel rapidly across organisational boundaries.

For commercial organisations and public bodies alike, the challenge is not simply to anticipate the next shock. Many sources of disruption cannot be predicted with precision, and several may occur at the same time. The more important question is whether organisations can continue to deliver what matters most when normal assumptions no longer hold, and whether they can adapt quickly as conditions change.

Disruption also creates opportunity. AI, automation and better use of data can improve productivity, decision-making and service delivery. New technologies, delivery models and sources of capital can unlock growth and capability. The organisations that benefit most will be those able to pursue these opportunities while maintaining clarity over the dependencies, trade-offs and risks they create.

This is changing the conversation about resilience. Leaders need to understand the minimum combination of services, people, technology, data, suppliers and resources required to remain viable through severe disruption, where concentration and common points of failure sit, and what difficult choices may be required when resources are constrained. Resilience and adaptability increasingly need to be designed into how the organisation operates. And assurance over these risks and opportunities is in the spotlight.

This year, our document covers the following areas:

- **Macro risk landscape:** The geopolitical and economic forces shaping the operating environment.
- **Market shifts:** Structural shifts including technology, AI and workforce change.
- **Risk hot spots:** Areas where disruption is creating particularly important assurance questions, including organisational viability, supply chains and third parties, cyber risk and data governance.

We hope this year's Agenda helps you look beyond individual risks and consider how disruption may interact across strategy, operations and resilience. For Internal Audit and assurance leaders, the opportunity is to use this perspective to shape plans, engage in Board-room discussions, challenge assumptions, sharpen priorities and help organisations remain effective as conditions continue to 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.

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
People, culture and workforce: Adapting to the future of work	19

3 Section 3: Risk hot spots →

The minimum viable company: Protecting organizational viability through disruption	22
Managing external disruption – supply chain management and third-party risk management	27
Supply chain management	28
Third-party risk management	30
The changing shape of cyber risk	34
Data as an asset	39
Wider risk landscape	43

4 Section 4: Contact us and glossary →

Contact us	45
Glossary	47

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 technology, 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 technology, 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 the 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 simply 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.



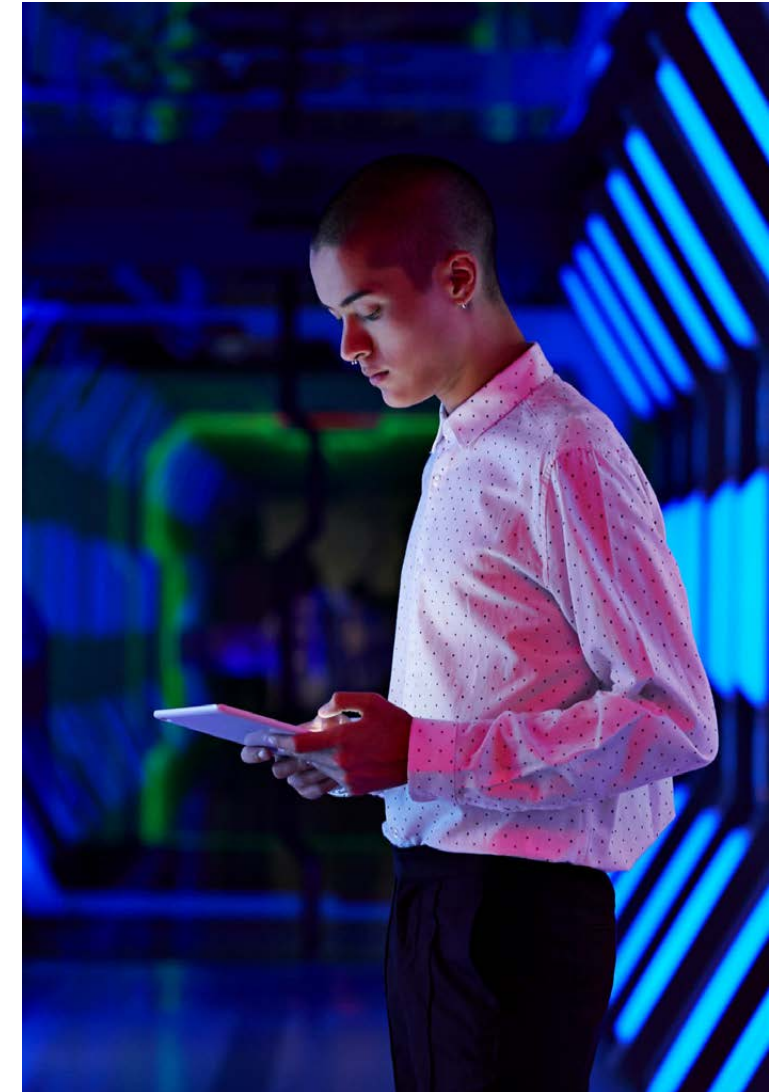
Internal Audit considerations

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.



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.

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.

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.

Six key trends are now shaping the future of work.

Technology: 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.

Capability: 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.

Experience and development: 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.

Careers: 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

Equality: 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?

Transparency: 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.



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. We have included a broader set of 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 hot spots



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.

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. Providers of critical national infrastructure also face particular challenges.

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 and internal capabilities (such as 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 security, technology recovery, crisis management, supply-chain resilience and emergency planning. Each may work in isolation, while the organisation lacks a single 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 disruption – supply chain management and third-party risk management



How should organisations adapt supply chain management and third-party risk management so that accelerating external disruption and innovation do not undermine delivery, trust or strategic progress?

No organisation can fully insulate itself from disruption. Geopolitical tension, trade fragmentation, tariffs, armed conflict, cyber threats and constrained access to energy and critical resources can quickly affect an organisation's ability to deliver. At the same time, rapid advances in AI and technology are creating new opportunities to improve performance and access capabilities beyond organisational boundaries. For leaders, the challenge is how to capture those opportunities and remain resilient when external conditions change.

Supply chain management and third-party risk management (TPRM) provide two complementary ways of responding. Supply chain management starts with the external supply network and asks whether it can continue to deliver and improve as conditions change. TPRM starts with the individual relationships on which the organisation depends: whether they remain appropriate, resilient and well managed throughout their lifecycle, and what those relationships collectively reveal about concentration, common dependencies and wider third-party risk.

Supply chain management

Supply chains are one of the principal channels through which external change affects organisational performance. Recent experience has seen geopolitical, cyber, resource and policy shocks arriving faster, interacting more readily and demanding decisions under greater uncertainty. Meanwhile, AI, analytics and automation have offered new ways to improve foresight, productivity and responsiveness.

Organisations are increasingly looking beyond sourcing and procurement efficiency. Business leaders want to know which products and services are genuinely critical, where the organisation is exposed to irreplaceable suppliers or resources, how much resilience is economically justified, and whether management can act quickly enough when conditions change. At the same time, the longstanding need to maintain responsible, ethical and sustainable supply chains remains important. These conditions are moving supply chain management ever closer to strategy, enterprise resilience and capital allocation.

Context: [Government Office for Science, Global Supply Chains: A Foresight report on risk and resilience \(15 June 2026\)](#)



Supply chain management

How leading organisations are adapting through supply chain management

Managing critical dependencies

01

Organisations are no longer treating every product, supplier and disruption equally. Instead, they are mapping critical outcomes to the materials, energy, technology, routes, facilities and specialist capability needed to deliver them. This supports more informed and prioritised decisions on inventory, sourcing, capacity, recovery and investment.

Improving end-to-end visibility and decision speed

03

Many organisations still rely on fragmented data, for example in spreadsheets and siloed functional reporting, making it difficult to see how operational, financial, cyber and geopolitical risks combine. As conditions change, organisations are investing in better data about dependencies, early-warning indicators and joined-up monitoring and decision-making, so that emerging constraints can be identified and acted on before delivery is affected.

Treating resilience as a measurable business choice.

05

Boards are increasingly challenging broad claims that a supply chain is resilient. Management is being asked to define tolerances, quantify the cost and benefit of resilience measures, and demonstrate that alternative suppliers, routes and workarounds can operate at the required scale and duration to withstand shocks and meet business needs. This shifts resilience from a general ambition to explicit choices about service, cash, inventory, capacity and risk.

Redesigning networks around resilience as well as cost

02

Business leaders are reassessing single-source dependencies, country and route concentration, long lead-time components and exposure to tariffs or export restrictions. The response is not universal nearshoring or excessive stock – it is targeted optionality: dual sourcing where it is viable, strategic buffers where substitution is slow, regionalisation where the risk justifies it, and clearer plans for constrained resources.

Using AI and analytics to strengthen judgement.

04

AI is increasingly supporting demand forecasting, scenario modelling, sourcing analysis, as well as identifying issues that require management attention. Organisations are moving beyond experimenting with AI and digital tools. Their focus is now more on whether the underlying data is reliable, whether model outputs are accurate and explainable, and where human judgement remains essential. The opportunity is faster and better decisions, the risk is accelerating poor assumptions or creating opaque allocation and sourcing choices.

Collaborating across ecosystems rather than organisational boundaries.

06

By ecosystems we mean the wider network of suppliers, contractors, technology providers, logistics partners, government and industry bodies that collectively enable critical outcomes. For critical infrastructure, public services, defence, energy transition and other capacity-constrained markets, no organisation can create resilience alone. Organisations are working more closely with strategic suppliers, government and sector partners to develop capability, improve information sharing, secure scarce resources and address systemic bottlenecks.

Supply chain management (continued)



Questions for leaders

- Which products, services and outcomes depend on resources, routes or suppliers that cannot be readily replaced?
- Where are the most material geographic, supplier, technology and resource concentrations across the end-to-end network?
- Can management detect and respond to disruption beyond Tier 1 suppliers early enough to protect critical operations?
- How are the conflicting demands of managing cost, cash, resilience, quality, timeliness, security, sustainability and reputation balanced in sourcing and network decisions?
- Are resilience investments supported by clear tolerances, scenarios and economic rationale?
- Have severe but plausible disruptions to suppliers, logistics routes, energy or critical resources been tested end-to-end?
- Where can AI materially improve foresight, planning and response, and where must human judgement remain decisive?

Internal Audit considerations

Internal Audit can assess whether supply chain management is helping the organisation achieve practical outcomes, not simply whether policies, processes and governance forums exist and are being applied. Reviews can focus on whether management has a sufficiently complete and decision-useful view of the external supply network and whether these insights are applied to inform sourcing, planning and resilience decisions.

Example topics include:

The methodology used to identify critical products, services, resources, routes and dependencies, including completeness beyond Tier 1.

The quality of demand, supply and scenario planning, including the assumptions used and the consideration of severe or concurrent disruption.

The design and governance of AI-enabled planning and sourcing, including data quality, explainability, human oversight and performance monitoring.

How the effectiveness of alternative suppliers, routes, workarounds and recovery arrangements has been demonstrated through testing or actual events.

Whether sourcing, inventory, capacity and substitution decisions reflect agreed risk appetite and resilience tolerances.

The use of early-warning information to enable timely decisions, clear escalation and coordinated action across procurement, operations, finance, risk and the business.

The integration of ethical sourcing, supplier conduct, sustainability and reputational exposure into supply-chain decisions.

Third-party risk management



Third-party risk management

Organisations increasingly rely on third parties for critical services, specialist capability, data, technology and innovation. Cloud providers, managed services, software platforms, AI vendors, contractors, alliances and contingent workforces can improve speed, flexibility and capability, but they also extend organisational risk boundaries. Even a relatively small provider has potential to create significant operational, cyber, data, regulatory or reputational risk exposure.

Business leaders are demanding more than mature onboarding processes and annual questionnaires to understand, assess and respond to third-party supply risks. The practical challenge is to identify which relationships matter most, apply proportionate controls throughout the lifecycle, detect material change quickly, and aggregate relationship-level information to understand concentration and common dependencies. TPRM is therefore evolving from a procurement checkpoint into a continuous management discipline that supports resilience, trust and responsible innovation.

Context: [NCSC, Supply chain security guidance](#)



How organisations are adapting through third-party risk management

- 01 Building a usable third-party universe.** Key to effective third-party risk management is the consolidation of fragmented supplier, contractor and partner records into a common taxonomy with clear ownership. The aim is not merely a complete list, it is a decision-useful view that connects third parties to the services, data, systems, sites and outcomes they support.
- 02 Prioritising by criticality and inherent risk.** Organisations are moving away from spend or organisational profile as proxies for risk. They are segmenting relationships according to the impact of failure, the sensitivity of information access, ease of access to substitutes, regulatory exposure and the nature of the service. This allows stronger controls and expert attention to be concentrated where risks are greatest.
- 03 Moving from periodic assessment to continuous lifecycle management.** Initial due diligence remains important, but risks can change materially once a contract is live. Organisations are using event-driven monitoring, external intelligence, performance data and clearer escalation triggers to identify changes in cyber posture, financial viability, compliance, ownership, geopolitical exposure and service performance.
- 04 Strengthening contracting and operational ownership.** Many TPRM weaknesses arise after approval because contractual rights are unclear or operational owners do not act on them. The imperative is now for organisations to set organisation-wide minimum information security, audit, incident, resilience, subcontracting and exit provisions by risk tier, while clarifying who monitors performance, accepts exceptions and leads remediation.
- 05 Understanding fourth parties and concentration.** Relationship-level assessments do not tell the full story if multiple critical providers depend on the same cloud platform, software component, data source, subcontractor, utility or specialist workforce. Organisations are increasingly aggregating third-party data to identify common dependencies and correlated failure risk that would otherwise remain hidden.
- 06 AI and other fast-moving services.** AI adoption by service providers raises questions about training data, intellectual property, model performance, explainability, security, misuse and human accountability. Organisations need to develop the skills and technical capability to identify, assess and challenge these risks, rather than relying on traditional third-party assessment approaches that may not be equipped to address them.
- 07 Focusing on outcomes and capability, not only framework compliance.** Boards increasingly want evidence that TPRM prevents disruption, improves supplier decisions, supports innovation and enables timely intervention. Organisations are therefore simplifying low-value questionnaires, automating routine checks and using skilled challenge on material relationships, control gaps and emerging risks.

Third-party risk management (continued)

The key risks and opportunities

01 An incomplete or unusable third-party view

Inconsistent definitions and disconnected systems prevent organisations from knowing which parties support critical services or access sensitive assets. The opportunity is to improve the quality and usability of third-party information, progressively building a more risk-based view that supports management action rather than a static inventory.

02 Controls that stop at onboarding

Generic due diligence and annual reviews do not keep pace with changing cyber, AI, financial, geopolitical and performance risks. The opportunity is to extend oversight beyond onboarding, using more timely and event-driven information to identify material risks, changes and issues requiring management intervention.

03 Innovation outpacing assurance

New AI, data and platform relationships can become critical before standard TPRM processes have adapted. The opportunity is to adapt assessment approaches as new services emerge, bringing together the right commercial, risk and technical expertise without unnecessarily slowing innovation.

04 Concentration hidden below relationship level

Individually acceptable providers may share common fourth parties or infrastructure. 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.

05 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.

06 Insufficient people and technical capability

TPRM programmes often depend on a small number of experienced individuals who lack the range of cyber, data, AI, operational or commercial expertise needed to challenge complex providers. The opportunity is to broaden capability over time, reduce reliance on key individuals and make better use of scarce specialist skills on the relationships and risks that most need them.

07 Supplier conduct and reputation

Labour practices, human rights, environmental performance and subcontractor behaviour can create reputational and legal exposure even where service delivery remains stable. The opportunity is to strengthen how responsible sourcing and supplier conduct are considered in ongoing monitoring, decision-making and remediation.

Third-party risk management (continued)



Questions for leaders

- Do we have a complete, consistently classified and decision-useful view of third parties, and do we know which support critical services, data and technology?
- Are due diligence and ongoing monitoring processes proportionate to criticality and inherent risk, rather than spend or organisational visibility?
- Can we identify common fourth parties and concentration across cloud, software, data, logistics and other shared providers?
- Do contracts provide workable information, security, audit, incident, resilience, subcontracting and exit rights, and are those rights used in practice?
- Are material changes, incidents and deteriorating performance escalated quickly enough for the business to act?
- Does the organisation understand where third parties are using AI to deliver products and services, and are the resulting risks around data, model performance, resilience, misuse and accountability being effectively managed?
- Does the organisation have sufficient commercial and technical capability to challenge critical providers or is there excessive reliance on a small number of key individuals?
- Can management demonstrate that TPRM is improving decisions, preventing disruption and enabling responsible adoption of external capability?

Internal Audit considerations

Internal Audit should move beyond confirming that a TPRM framework exists. Its work should determine whether the discipline is producing demonstrable outcomes: better supplier selection, stronger oversight of critical relationships, earlier identification of change, greater readiness to respond to incidents, more informed use of external innovation and a clearer enterprise view of dependency and concentration.

The completeness, accuracy and practical use of the third-party inventory, taxonomy, ownership model and criticality assessment.

Whether controls are proportionate by risk tier and operate throughout onboarding, contracting, service delivery, renewal, change and exit.

The quality and timeliness of continuous monitoring, issue management, exception approval and escalation, including whether signals result in action.

Whether contractual standards are adequate and operationally usable, and whether management understands where key rights or protections are absent.

The organisation's ability to identify fourth parties, common providers and concentration risk and to translate that insight into continuity or substitution strategies.

The treatment of AI, cloud, data and other technology providers, including multidisciplinary challenge and clear accountability for residual risk.

Whether key-person dependency and capability gaps in TPRM, procurement and technical specialist functions undermine effective challenge.

Integration with supply chain management, operational resilience, cyber, data governance, responsible sourcing and enterprise risk without duplicating activity.

Whether management information distinguishes completed process steps from real outcomes, such as reduced exposure, timely remediation and tested resilience.

Managing external disruption – supply chain management and third-party risk management

Bringing the two disciplines together



Supply chain management and TPRM should not be collapsed into one discipline, but neither should they operate in isolation.

Supply chain management starts with the system: the flows, resources, routes and capabilities needed to deliver.

TPRM starts with the relationship: whether each relevant third-party is appropriately selected, contracted, monitored and exited.

The strongest organisations connect the two views so that relationship-level information informs systemic resilience decisions whilst systemic priorities determine where the deepest third-party management is required.



For Internal Audit, the implication is equally practical. Assurance should test not only whether frameworks and controls are well-designed, but whether these disciplines are enabling informed decision-making, protecting critical outcomes and enabling the organisation to use external innovation with confidence.



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



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 cyber security matters

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

Customers, regulators, investors and supply chain partners are all asking hard 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 on now (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 on now (continued)

The key risks and opportunities

Old assets, new exposure

Many operational technology environments depend on long-life assets built with a focus on 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

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

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

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

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

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



Data as an asset

Why data governance matters

Data is now widely recognised as one of an organisation's most important assets, underpinning decision-making, operational performance and innovation. However, the growing volume, complexity and regulatory expectations associated with data can make effective management challenging.

Whilst AI is dominating the agenda on data, several long-term trends continue to grow.

01 More data, moving faster and across more environments

Organisations are generating, acquiring and sharing data across cloud platforms, applications, third parties, AI models and connected ecosystems. The challenge is no longer simply storing data, but maintaining its quality, meaning and control as it moves.

02 Trusted data is becoming fundamental to business strategy

Accurate reporting, operational decisions, regulatory submissions, analytics and AI increasingly depend on data that is complete, accurate, timely and understood.

03 Competitive advantage depends on the ability to use data responsibly

Organisations able to discover, combine and use trusted data quickly are better positioned to innovate, automate and respond to changing customer and market needs.



Data governance is therefore shifting from a compliance activity to a business capability that enables trusted reporting, decision-making and AI.

The key risks

Poor data quality

Inaccurate, incomplete, inconsistent or outdated data can undermine management and regulatory reporting, business decisions, analytics and AI outputs.

Unclear ownership and accountability

Gaps in responsibility can lead to weak controls, unresolved issues and inconsistent data management.

Inappropriate access or use

Sensitive or personal data may be accessed, shared or used beyond its intended purpose.

Limited data lineage and traceability

Organisations may be unable to determine where critical data originated, how it was transformed, which controls were applied and whether it remains appropriate for its intended use.

Unmanaged access

Inadequate controls over how data is accessed and protected can lead to regulatory breaches, cyber incidents, data loss and reduced organisational control.

Excessive retention and data proliferation

Unnecessary duplication and retention increase cost, complexity, exposure and compliance risk.

Loss of confidence and trust

As organisations depend on data for more important decisions, the consequence of data failure increases. Data risk is therefore increasingly a business risk rather than simply a technology or compliance risk.

Data as an asset (continued)

The opportunities

Data is increasingly featured at the heart of corporate strategy with business leaders citing the data they hold as a source of competitive advantage and an enabler of next-generation products and services.

More data, more risks?

As organisations create, acquire and rely on more data, their exposure to data-related risks inevitably increases. Risks that were once confined to specialist teams now have the potential to affect operations, finances, customers and organisational reputation.

Effectively managing these risks is critical if organisations are to realise the value, efficiencies and innovation often used to justify investment in data transformation.

By governing data differently, the risks can be better managed and opportunities realised.

The key trends shaping data governance priorities

Historically, data governance programmes were largely driven by regulatory and control requirements, with a focus on ownership, quality, security and privacy.

These remain fundamental, but modern governance

increasingly balances control with enablement: Protecting critical data while allowing the organisation to access, share and use data quickly for reporting, analytics, innovation and AI.

Greater emphasis on local accountability

- Clear ownership remains one of the most significant success factors for effective data governance. Accountability is being strengthened through defined roles such as Data Owners, Data Stewards and Data Custodians, with responsibilities for data quality, discoverability, access, lifecycle management and compliance.
- Increasingly, governance is extending beyond IT, with business functions taking greater ownership and management of the data they create and rely upon. Central data governance teams are increasingly tasked with providing tooling and structures to enable business-led data management.

Automation and continuous monitoring

- Manual governance activities are increasingly being supplemented by automation. Examples include automated data classification, the automatic collection of information about data assets, continuous monitoring of data quality, visibility of where data comes from and how it moves through systems, and automated enforcement of governance policies.
- Continuous monitoring provides greater visibility of control effectiveness and enables the identification of issues before they become material business risks.

Data governance as an enterprise capability

- Rather than being viewed as a standalone control function, data governance is increasingly being embedded across business operations.
- There is a move away from governance programmes that focus solely on policy documentation towards governance that is integrated into day-to-day decision-making, delivery and operational processes. This reflects a recognition that governance should enable the effective use of data rather than restrict it.

Data as an asset (continued)

Data is now created and consumed continuously across cloud platforms, APIs, analytics and AI. Annual reviews and policy documents alone cannot provide enough assurance, controls need to be embedded, automated and evidenced as data is used.

Key features of modern data governance

Business-owned data with federated accountability - Domains own the data they create and use, with Data Owners and Stewards accountable for quality, definitions, access and lifecycle decisions, central teams set standards and enable.

Policy translated into executable controls - Governance standards become executable rules in data pipelines, products and approval workflows, creating consistent controls and an auditable evidence trail.

System-enforced data access, retention and disposal - Access, purpose, retention and deletion requirements are built into platforms and pipelines, reducing reliance on people remembering and applying policy manually.

Governance platforms connecting business and data teams - Catalogues, definitions, lineage, ownership, controls and issues are brought together so users can find trusted data while the data office maintains enterprise oversight.

Continuous monitoring of data quality and controls - Quality, lineage, usage and control health are monitored continuously, helping confirm that data remains reliable for regulatory reporting, analytics and AI use.

Real-time quality, control and risk alerts - Rules monitor critical fields, anomalies and control failures as data moves, alerting owners before inaccurate reporting, operational decisions or AI outputs are affected.

Automated data discovery and labelling - Metadata scanning and AI-assisted classification identify new data, apply business and sensitivity labels and keep catalogues current with less manual effort.

Questions for leaders

Do we have clear, named ownership for the data that matters most - and are those owners empowered and held accountable for quality, access and lifecycle decisions?

Are our governance policies enforceable through technology, or do they still rely primarily on people reading documents and following prescribed rules? Where technology automates controls, are they suitably configured and can they be by-passed?

Can we demonstrate that access, retention and disposal controls operate automatically across our data estate - or would a review find material gaps between policy and practice?

Can our people find, understand and trust the data they need - and does the data office have enterprise-level visibility of ownership, quality, lineage and control health?

Are we monitoring data quality and control effectiveness continuously, or do we still rely largely on periodic reviews and annual attestations?

Would we know quickly enough if critical data became inaccurate, incomplete or compromised - before it affected a regulatory submission, business decision or AI output?

Do we have confidence that new data entering the organisation is being identified, classified and brought under governance - or are there material blind spots?

Data as an asset (continued)

Trusted data now underpins accurate reporting, AI-enabled decisions and operational control.

Modern governance is therefore moving from document-led oversight to business-owned controls embedded in data products, workflows and technology.



The outcome

Data that is findable, understood, trusted, protected and reusable safely at speed.

Internal Audit considerations

As data becomes more dynamic, interconnected and important to reporting and AI, governance can no longer rely primarily on policies and periodic review. Controls increasingly need to operate where data is created, changed, accessed and used.

This also changes assurance. Rather than primarily assessing whether policies and controls have been designed, Internal Audit will increasingly be able to examine evidence of how controls are operating across data environments in near real time.

How assurance over data risk is evolving:

Yesterday:

Data governance through human review of observed documents

Historically, organisations created:

- Policies
- Standards
- Procedures
- Annual attestations
- Training

This approach expected people to read documents and follow prescribed rules. Internal Audit reviews looked at the design of these documents as a measure of control.

This worked well when data volumes were smaller, systems were fewer, and data movement was relatively well understood.

Today:

Data governance by process and workflows

Organisations today face an evolving data landscape – cloud platforms, AI models, real-time data pipelines, API integrations, large-scale data sharing and complex architectures.

How we use the data has changed, along with a dramatic increase in data-related regulation over the last 10 years.

Manual, policy-led governance is increasingly unable to keep pace with the scale, complexity and speed of modern data environments.

Tomorrow:

Governance by technology, administered by the end user

The future of data governance is not more policies, but the translation of policy content into automated, measurable and continuously monitored controls that are integrated into technology and business processes.

Governance by design will support AI, real-time monitoring and faster, more responsible use of data at scale.

This changes how assurance leaders review and inspect controls to manage data risk.

Data as an asset (continued)

Internal Audit considerations (continued)

For assurance leaders, the shift to modern data governance means assurance needs to move beyond reviewing whether policies and frameworks exist, toward testing whether governance is actually operating effectively across the data estate.

Show me, don't just tell me

Observe the outcomes

Design assurance for automated controls

Test the logic, configuration, exception handling and monitoring of automated controls and confirm that there remains appropriate human oversight.

Test outcomes, not just design

Use data-led testing to validate whether ownership, quality, access, retention and other controls are operating as intended.

01

02

04

03

Prioritise critical data and use cases

Focus assurance on the data that supports material decisions, regulatory obligations, customer outcomes and high-risk AI applications rather than attempting equal coverage of the entire data estate.

Assess governance where it happens

Review controls embedded within data platforms, workflows, cloud environments and AI solutions rather than relying solely on central governance documentation.

Risk landscape – Commercial and Government

- **Strategy and financial sustainability**
Strategic delivery, financial sustainability, cost reduction, productivity, demand pressures, scenario planning.
- **Major programmes and transformation**
Programme delivery, benefits realisation, digital transformation, operating-model redesign, portfolio prioritisation.
- **Commercial and procurement**
Procurement, contract management, supplier performance, sourcing strategy, commercial capability, value for money.
- **Third-party and supply-chain risk**
Critical suppliers, supply-chain concentration, supplier failure, geopolitical dependencies, resilience, subcontractors.
- **Operational and service resilience**
Technology architecture, legacy technology, cloud, change and release management, data quality, regulatory data, AI/model-enabled processes.
- **Technology and legacy systems**
Legacy technology, cloud, technology modernisation, systems integration, technical debt, change management.
- **Cyber and information security**
Ransomware, nation-state threats, identity and access, vulnerability management, recovery, security monitoring.
- **Data and information governance**
Data quality, records, information management, data sharing, privacy, management information, analytics.
- **Fraud and economic crime**
Procurement fraud, grant fraud, payroll fraud, insider fraud, bribery and corruption, conflicts, fraud risk assessment.

- **Governance and accountability**
Board/committee effectiveness, delegated authorities, decision-making, risk management, assurance mapping, accountability.
- **Workforce and capability**
Skills shortages, workforce planning, key-person dependencies, contingent labour, succession, organisational culture.
- **People and conduct**
Speak-up, ethics, conflicts of interest, health and wellbeing, behavioural risk, performance and incentives.
- **Regulatory and legal compliance**
Sector regulation, statutory obligations, corporate reporting, litigation, legal compliance, policy implementation.
- **Assets, estates and infrastructure**
Asset condition, maintenance, capital programmes, health and safety, physical security, estate optimisation.
- **Health, safety and safeguarding**
Workforce safety, public/user safety, safeguarding, duty of care, incident management, contractor safety.
- **Sustainability and climate resilience**
Net zero, climate adaptation, physical risks, sustainable procurement, environmental compliance, transition plans.
- **Partnerships and delivery models**
Joint ventures, arm's-length bodies, grants, partnerships, shared services, outsourced delivery.
- **Geopolitical and national-security risk**
Critical supply chains, foreign influence, sanctions, sensitive assets, economic security, strategic dependencies.

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:



Stephanie Edenborough

UK C&G Internal Audit Leader

Partner

+44 (0) 7834 254 859

stephanie.edenborough@pwc.com



Helen Morris

UK Internal Audit

Director

+44 (0) 7725 445 148

h.morris@pwc.com



Anoop Gandhi

Technology Internal Audit

Director

+44 (0) 7841 570 689

anoop.g.gandhi@pwc.com



Bobbie Ramsden-Knowles

UK Crisis and Resilience Leader

Partner

+44 (0) 7483 422 701

roberta.ramsden-knowles@pwc.com

Glossary of acronyms and abbreviations

AI/ML/DL	Artificial Intelligence/Machine Learning/Deep Learning	IBS	Important Business Services
AML	Anti-Money Laundering	IMF	International Monetary Fund
API	Application Programming Interface	IPO	Initial Public Offering
BCM	Business Continuity Management	IoT	Internet of Things
BoE	Bank of England	IT	Information Technology
CEO	Chief Executive Officer	KYC	Know Your Client
CFO	Chief Financial Officer	MI	Management Information
CIF	Critical or Important Functions	MTP	Material Third Party
EU	European Union	MVC	Minimum Viable Company
FRC	Financial Reporting Council	NCSC	National Cyber Security Centre
GDP	Gross Domestic Product	NIST	National Institute of Standards and Technology, United States
HM	His Majesty	OT	Operational Technology
HMT	His Majesty's Treasury	PQC	Post-Quantum Cryptography
HVAC	Heating, Ventilation and Air-conditioning	SDR	Sustainability Disclosure Requirements

Glossary of acronyms and abbreviations (continued)

TPRM	Third-Party Risk Management
UK	United Kingdom
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.