

Internal Audit in 2027:

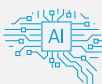
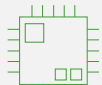
where assurance can have
the greatest impact



Where should Internal Audit focus next?

Not every emerging risk belongs on the audit plan. The challenge is to identify where rapid change, uncertainty and growing dependency have created a gap between what an organisation believes is controlled and what is happening in practice. For Internal Audit, the question is no longer simply what new risks are emerging, but where assurance can have the greatest impact.

Seven areas of focus for Internal Audit in 2027

01		AI, automation and accountability
02		Cyber resilience
03		Geopolitical and economic uncertainty
04		Operational resilience and critical dependencies
05		Third-party dependencies and concentration risk
06		Information integrity and digital trust
07		People, culture and skills

A changing risk landscape

- The challenge for 2027 is not identifying new risks. Most organisations already have a good understanding of the issues that could affect their objectives. The harder task is deciding where assurance is needed most and ensuring that audit coverage keeps pace with a changing risk landscape. Artificial intelligence (AI) is changing how work is done and how decisions are made. Cyber threats continue to develop. Geopolitical tension is affecting trade, regulation and supply chains. At the same time, many organisations are cutting costs, changing operating models and relying more heavily on a small number of technology and service providers. These risks are converging rather than developing in isolation. A cyber incident may start with a third party, interrupt a critical service, expose poor data governance and create regulatory consequences. A cost programme may deliver its savings while quietly removing experienced staff or weakening important controls. An AI tool may improve productivity but introduce new data, fraud and accountability risks.
- The 2027 audit plan should therefore be selective rather than simply longer. It should focus on where risks converge, where dependencies could transmit disruption across the organisation and where management and the Board have the least reliable assurance. Internal Audit can add value by helping Boards understand not only whether controls are operating effectively, but whether management is responding to change quickly enough. In many organisations, the challenge is not a lack of information, but whether management information is timely, reliable and capable of supporting effective decision-making. Strong governance depends as much on the quality of information available to decision-makers as it does on the controls themselves.
- These themes are particularly relevant to Irish organisations operating within a highly open economy, an increasingly complex EU regulatory environment and interconnected international supply chains. The ability to anticipate disruption, adapt quickly and maintain trust has become important across both the public and private sectors.

01

AI, automation and accountability

AI in everyday operations

By 2027, many organisations will have moved beyond small AI trials. AI will increasingly be embedded within day-to-day operations, existing software platforms and third-party services, influencing how decisions are made, information is analysed and customers are served. The challenge is that organisations may be using AI without fully understanding where it operates, which data it uses or who remains accountable for the resulting decisions and outcomes.

AI governance and accountability

Governance must extend beyond the approval of standalone AI tools. Management needs visibility over AI developed internally, accessed by employees or embedded within supplier platforms and business applications. The risks increase as AI moves from assisting employees to recommending, initiating or making decisions, particularly where those decisions affect customers, financial reporting or regulatory obligations. For Internal Audit, the focus should be less on the existence of AI policies and more on whether governance reflects how AI is being used in practice. Reviews should assess whether management has sufficient visibility over AI use, whether controls are proportionate to the risks involved and whether appropriate oversight exists where AI influences decisions or business outcomes. Reviews should also determine whether human oversight is meaningful in practice. A process described as “human in the loop” may provide limited protection if employees lack the information, time, expertise or authority required to challenge an AI-generated output. Internal Audit should apply the same discipline to its own use of AI. Technology can support planning, analysis and reporting, but responsibility for evidence, judgement and conclusions remains with the auditor.

What this means for you

Organisations must understand where AI is being used, who is accountable for its outputs and whether effective oversight is in place.

02 Cyber resilience

Cybersecurity remains a core audit priority

Cybersecurity remains a core audit priority, but the discussion is increasingly moving beyond prevention. Organisations must be able to detect, contain and recover from incidents in an environment where AI enabled impersonation, deepfakes, ransomware and supplier compromise continue to evolve.

Concentration risk can be hidden

Attention should also extend to operational technology and connected infrastructure, concentration in cloud and technology providers, and the longer-term implications of quantum computing for the cryptography underpinning data security and digital trust.

Focus on recovery and response

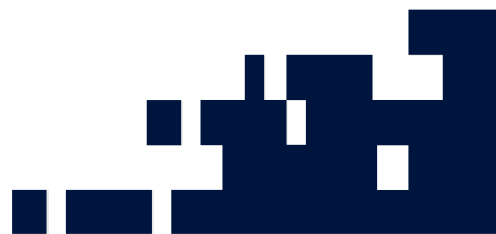
The most significant cyber failures often occur not because controls are absent, but because organisations struggle to respond effectively when incidents occur. Boards need confidence that recovery arrangements, communications and decision-making processes will operate effectively under pressure.

Testing preparedness and control effectiveness

Internal Audit can help assess whether organisations are prepared to respond to and recover from a cyber incident, rather than simply demonstrating that controls exist. Reviews should focus on whether critical controls, response arrangements and recovery plans would remain effective during a cyber event.

What this means for you

Internal Audit should assess whether organisations can respond to and recover from cyber incidents, not just prevent them.



03

Geopolitical and economic uncertainty

Geopolitical and economic pressures

Tariffs, sanctions, export controls, conflict and competition for critical resources are changing costs, markets and supply chains. Organisations do not need to operate directly in affected regions to experience disruption. Exposure may sit with customers, suppliers, technology providers or assumptions built into strategic plans.

Indirect financial and operational impacts

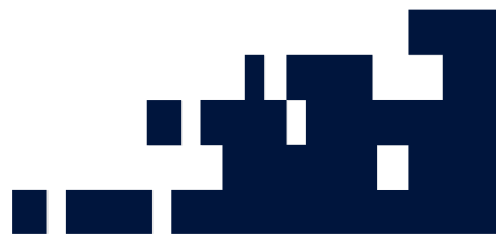
Financial pressure can also create risk indirectly. Cost reduction targets, refinancing pressures and weaker trading conditions may encourage optimistic forecasting, management override or underinvestment in important control and resilience activities. These issues may not justify a standalone audit in every organisation, but they should influence risk assessments and audit planning decisions.

Focus on assumptions and dependencies

Internal Audit should consider these pressures when scoping reviews of strategy, financial planning, procurement, supply chains, third-party management and operational resilience. The objective is not to predict geopolitical events, but to assess whether material assumptions and dependencies are understood, monitored and linked to practical management actions. Scenario planning should identify decision points, accountable owners and the indicators that would trigger a change in approach

What this means for you

Internal Audit should challenge whether critical assumptions and dependencies remain valid.



04

Operational resilience and critical dependencies

Understanding critical dependencies

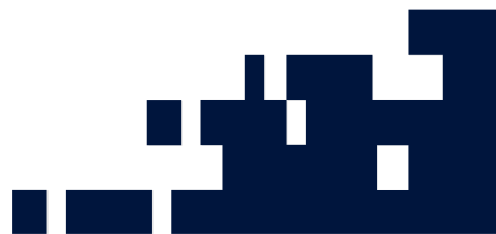
Business continuity documentation does not, by itself, demonstrate resilience. Organisations need a clear understanding of how critical services are delivered across people, premises, technology, data, utilities and suppliers. Weaknesses often emerge in the connections between those components rather than within individual controls. The more important question is whether management genuinely understands what critical services depend on and how those services would operate during a significant disruption. Management should also understand the minimum combination of services, people, technology, data and suppliers that the organisation would need to preserve if normal recovery arrangements were overwhelmed, including what could be stopped, degraded or deferred. Resilience testing should involve realistic scenarios and difficult decisions rather than simply validating that plans exist. Actions arising from incidents and exercises should address root causes and be independently verified before closure

Testing resilience under pressure

Internal Audit can add value by assessing whether management has visibility of critical dependencies and whether recovery assumptions remain realistic if several services fail simultaneously. The focus should be on the organisation's ability to continue delivering critical services rather than simply maintaining resilience documentation.

What this means for you

Internal Audit should challenge whether critical services can continue when key dependencies fail.



05

Third-party dependencies and concentration risk

Growing reliance on third parties

Organisations are becoming increasingly dependent on third parties, cloud providers and specialist service providers. The most important dependency is not always the largest contract. Smaller suppliers may support critical controls, hold sensitive information or provide services for which there are limited alternatives.

Identifying hidden concentration risk

Concentration risk can also be hidden. Different suppliers may rely on the same cloud platform, technology provider or subcontractor, creating dependencies that are not immediately visible. As organisations increase outsourcing and digitalisation, these risks become more significant.

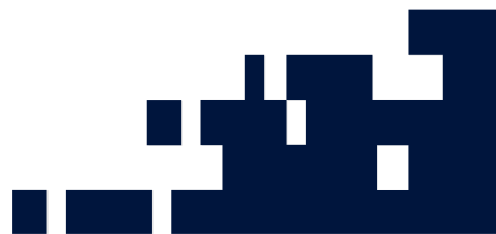
Strengthening third-party assurance

For Internal Audit, the real test is not simply whether a third-party risk-management framework exists, but whether it changes sourcing, contracting, monitoring and resilience decisions. Reviews should focus on critical dependencies, common fourth parties, concentration risk, continuous monitoring and the credibility of contingency, substitution and exit arrangements. The central question is whether management can move from supplier, to service, to dependency, to business impact and, ultimately, to timely action.



What this means for you

Internal Audit should challenge whether critical supplier dependencies and concentration risks are adequately managed.



06

Information integrity and digital trust

Building confidence in critical information

Organisations increasingly need confidence not only that information is accurate, but also that it is authentic, complete and produced through a trusted process. AI, automation, regulatory reporting and management decision-making all depend on reliable information. Yet ownership, definitions and lineage often remain unclear until information is needed for an important decision or external submission. At that point, inconsistencies and control weaknesses can become difficult to address quickly.

The growing risk of unreliable information

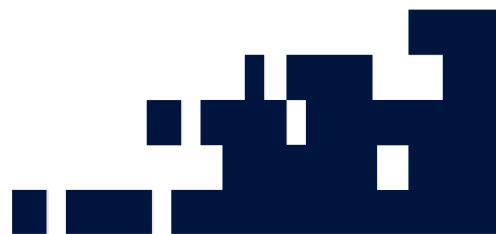
The reliability of information is increasingly becoming a risk. Synthetic documents, voice cloning and deepfake technology can be used to impersonate executives, alter evidence and support fraudulent transactions. Regulatory expectations around data, AI and public disclosures also continue to increase, requiring organisations to support key decisions with reliable information and evidence.

Focusing assurance on decision-critical information

For Internal Audit, assurance should focus on the information that supports material decisions, regulatory obligations, public reporting and higher-risk AI use rather than attempting equal coverage of the entire data estate. Reviews should assess ownership, quality, lineage, access, retention and change controls, while also considering whether the authenticity of critical documents, communications and transactions can be established. Fraud prevention, data governance and information integrity can no longer be considered in isolation.

What this means for you

Internal Audit should assess whether critical information is accurate, reliable and can be trusted.



07

People, culture and skills

Skills requirements are changing

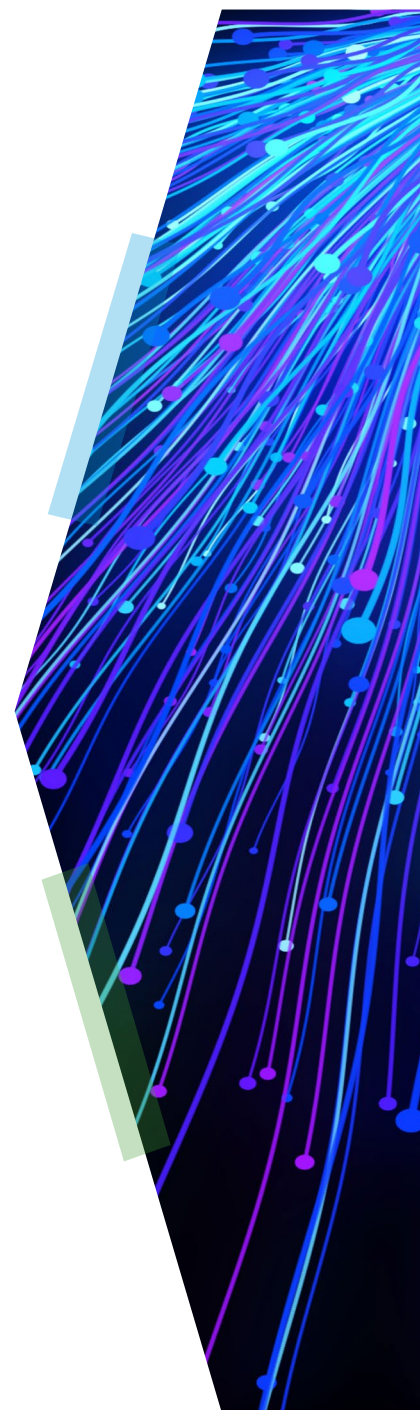
AI, automation and changing workforce expectations are reshaping organisational roles at a rapid pace. Many organisations continue to face shortages in technology, cyber, data and regulatory skills while simultaneously managing restructuring, succession risk and workforce change.

Future skills and capability gaps

There is also a risk that organisations automate entry-level work without considering how future professionals develop judgement, scepticism and practical experience. Without deliberate changes to career pathways and development, this may create capability gaps that only become visible after experienced employees have left the organisation.

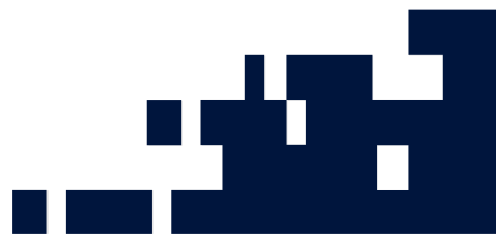
Assessing culture, capability and succession

Internal Audit should look beyond engagement surveys and policy statements. Culture is reflected in decisions, incentives, escalation and accountability. Reviews should consider whether performance measures encourage the right behaviours, whether concerns are raised and acted upon, whether succession plans exist for critical roles and whether key knowledge is concentrated in a small number of individuals. Internal Audit is not immune to these pressures and should also assess whether it has the skills and capacity required to provide assurance over emerging and increasingly complex risks.



What this means for you

Internal Audit should assess whether culture, skills and succession planning are sufficient to support organisational resilience and future needs.

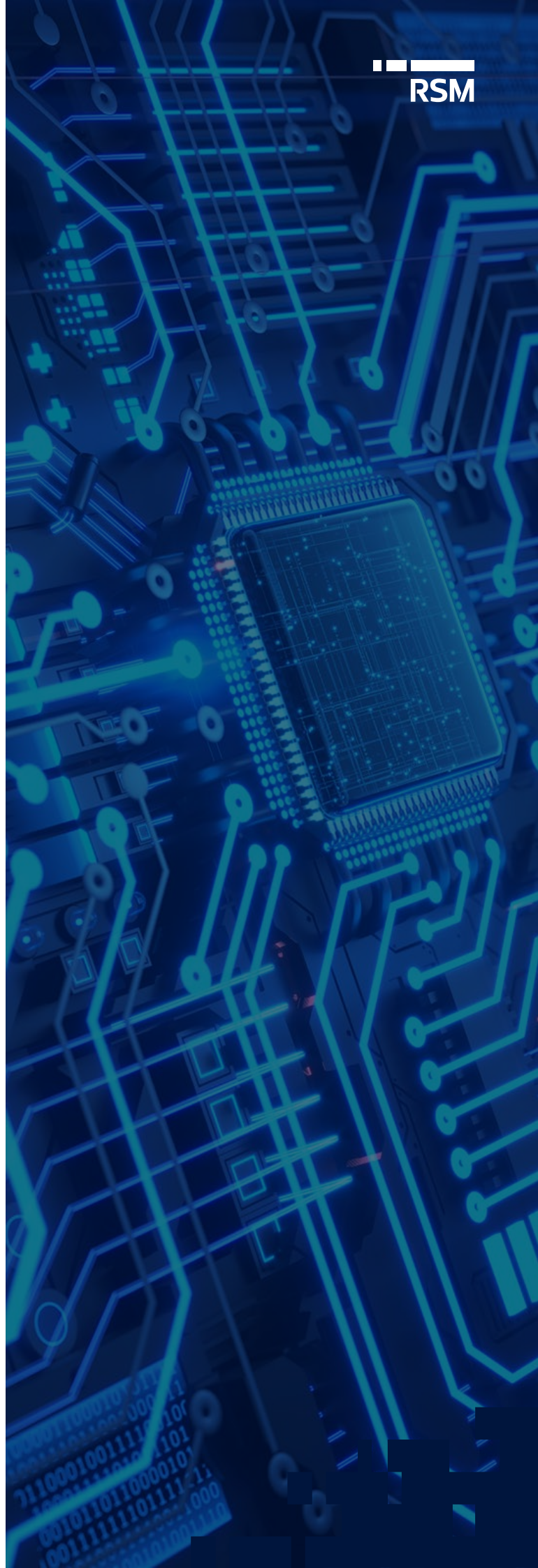


What should change in the 2027 audit plan?

Most organisations already maintain extensive risk registers and audit universes. The challenge is deciding where assurance is likely to make the greatest difference. Audit plans should focus on:

- 1 Areas where uncertainty is increasing.
- 2 Critical dependencies that could transmit disruption across the organisation.
- 3 Risks that are converging and could have wider consequences if they materialise.
- 4 Assurance gaps where management and the Board have limited visibility.
- 5 Emerging issues where early engagement can prevent weak controls becoming embedded.
- 6 Maintaining flexibility to respond as risk profiles change.

The strongest Internal Audit functions in 2027 will not be those with the largest audit plans. They will be those that understand where risk is changing, where risks are converging and where assurance can have the greatest impact.



The RSM team



Colm Laird

Partner, Risk and Governance
colm.laird@rsmireland.ie



Catherine Keenan

Associate Director
catherine.keenan@rsmuk.com



Ian McCartney

Consulting Director
ian.mccartney@rsmuk.com



Syed Haque

Director, Audit
syed.haque@rsmireland.ie



Ann Marie Conroy

Senior Manager, Risk and Governance
annmarie.conroy@rsmireland.ie



Divan Steyn

Senior Manager, Risk and Governance
divan.steyn@rsmireland.ie



Sive Riznyczok

Senior Manager, Risk and Governance
sive.riznyczok@rsmireland.ie



Mohit Khanduja

Manager, Risk and Governance
mohit.khanduja@rsmireland.ie



Yevgen Shuvalov

Consultant, Risk and Governance
yshuvalov@rsmireland.ie



Barney Doyle

Managing Consultant
barney.doyle@rsmuk.com

RSM Ireland Business Advisory Limited

Block D, Iveagh Court,
Harcourt Rd,
Dublin 2,
D02 VH94
T +353 (0)1 496 5388
www.rsmireland.ie

RSM Ireland Business Advisory Limited is a member of the RSM network and trades as RSM Ireland. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm which practises in its own right. The RSM network is not itself a separate legal entity in any jurisdiction. Directors: Niall May, Michael Mulholland and Paddy Stapleton.

RSM Ireland is a trading name of RSM Ireland Business Advisory Limited which is authorised by Chartered Accountants Ireland to carry on investment business.

RSM Ireland Business Advisory Limited (506769) is a private company limited by shares, registered in Ireland. Registered address: Fifth Floor, Block D, Iveagh Court, Harcourt Rd, Dublin 2, D02 VH94, Ireland.

The network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 200 Aldersgate Street, Upper Ground Floor South, London, EC1A 4HD. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.