RISK in FOCUS

2026/ 2027

Hot topics for internal auditors

INTERIM REPORT

CONTENTS

EXECUTIVE SUMMARY

Risk in Focus 2026/27 is a flagship study, now in its eleventh edition, offering forward looking insight into the risks organisations across Europe and the UK expect to face and how internal audit functions are responding.

This year's survey has been enhanced to gain greater insight into risk severity, maturity and internal audit assurance coverage and proportionality to the risk.

This interim report provides an early view of the survey results from 797 Chief Audit Executives (CAEs) and senior internal auditors, highlighting where perceived risk, risk severity, risk management maturity and internal audit attention appear well aligned—and where they do not. Details regarding the methodology, participants and survey questions can be found in the appendices.

Across the data, cybersecurity and data security remains the dominant risk and the only area where internal audit effort is fully aligned with risk ranking. However, alignment is not automatically evidence of risk driven planning, particularly where regulatory pressure and stakeholder expectations are strong and where risk management maturity is comparatively higher. In contrast, macroeconomic, social and geopolitical uncertainty and digital disruption/new technologies/AI combine high severity with some of the lowest maturity scores and persistently weaker audit coverage, suggesting growing blind spots and a need for more governance focused, capability building and resilience testing audit approaches.

The survey findings suggest many internal audit plans remain anchored in traditional, compliance driven topics (for example, governance/reporting and fraud) while externally driven and harder to audit risks receive less attention. They also indicate that some regulatory developments (including DORA and NIS2) may be "absorbed" into cyber and digital categories, potentially obscuring the true level of regulatory pressure. The headline findings below summarise the most material patterns for audit planning and assurance strategy.

INTERPRETING THE RESULTS: BLIND SPOTS, ANCHORS AND WHAT "ALIGNMENT" REALLY MEANS

Across the seven survey questions, a consistent pattern emerges for macro/ geopolitical uncertainty, digital disruption/ AI and (less visibly) market change: respondents rate these risks as highly important and severe, yet place them near the bottom for risk management maturity and relatively low for internal audit effort, coverage and proportionality.

Taken together, this points to potential blind spots—particularly where risks are externally driven, fast moving and difficult to express as traditional, checklist style audits.

The data also reinforces how interconnected these exposures are: macro and geopolitical shocks can cascade into cyber vulnerability, supply chain disruption, liquidity pressure and market volatility. If audit plans treat risks in isolation, they may underestimate compound risk and overestimate assurance. This strengthens the case for more outcome focused work that tests governance, decision making, resilience and preparedness (including operational resilience and crisis management), alongside capability building assurance in low maturity domains such as AI.

At the same time, many plans appear anchored in familiar, compliance driven areas: regulations, fraud and governance attract relatively high attention despite lower risk ranking. The reduced prominence of "new and changing laws and regulations" therefore warrants scrutiny; developments such as DORA and NIS2 may be absorbed into cyber and digital categories, making regulatory pressure less visible as a standalone driver. Finally, while cybersecurity shows the closest alignment between perceived risk and audit effort, alignment alone is not proof of a risk driven plan—particularly where maturity is higher and coverage may also reflect regulatory, stakeholder and second line reliance factors.

← BACK NEXT → CONTENTS

INTERPRETING THE RESULTS: BLIND SPOTS, ANCHORS AND WHAT "ALIGNMENT" REALLY MEANS

The table brings these themes into sharper focus by summarising each risk's relative position across all seven questions. It enables a side by side comparison of risk exposure (ranking and severity), management capability (maturity) and internal audit response (effort, adequacy, proportionality and intended change). The observations that follow highlight the most material patterns for audit planning.

	Risk			Internal Audit Assurance			
Risk	Rank	Severity	Maturity	Effort	Coverage	Proportionate to risk	Coverage increased
Cybersecurity	1	1	2	1	3	7	2
Digital disruption	2	2	16	8	12	15	1
Macroeconomic	3	3	15	15	15	16	12
Laws and Regulation	4	5	7	2	6	4	5
Human Capital	5	6	12	9	11	12	8
Operational Resilience	6	4	9	3	5	5	3
Market Changes	7	7	8	14	14	14	14
Financial	8	11	1	5	1	1	10
Supply chain	9	8	10	7	7	9	4
Climate Change	10	14	14	12	13	8	11
Organisational culture	11	9	13	11	9	11	9
Reputation	12	10	5	13	10	10	16
Fraud	13	13	11	6	4	3	6
Organisational Governance	14	12	4	4	2	2	7
Health, safety and security	15	15	3	10	8	6	13
Mergers	16	16	6	16	16	13	15

This table summarises how CAEs ranked each risk category across the seven survey questions. 1st is the highest-ranked category and 16th the lowest-ranked.

INTERPRETING THE RESULTS: BLIND SPOTS, ANCHORS AND WHAT "ALIGNMENT" REALLY MEANS

Cyber is the clearest "all round priority": it ranks first for risk and severity and first for internal audit effort, with relatively strong coverage and increasing coverage intent. Maturity is also high (second), which makes it important to confirm the plan is calibrated to current threat and reliance on the second line—not simply maintained because of regulation and stakeholder expectation.

Digital disruption/AI is the clearest capability and assurance challenge: it ranks second for risk and severity but last for maturity, indicating significant governance and control build is still underway. Internal audit effort sits mid table and coverage/ proportionality remain low, although respondents indicate a shift is coming (ranked first for increasing coverage).

Macroeconomic/geopolitical uncertainty shows the starkest mismatch: it ranks third for risk and severity while maturity is last, and internal audit effort, coverage and proportionality cluster near the bottom. This suggests the exposure is widely recognised but not yet embedded in planning. Some assurance may be delivered indirectly through related work (for example, operational resilience, supply chain and governance), and the IIA topical requirement on organisational resilience may be helping to refocus audit attention on resilience and crisis management.

Human capital also shows misalignment: risk importance and severity remain relatively high while maturity is lower (12th), potentially reflecting recruitment pressures and the demand for new skills to support initiatives such as AI adoption. Internal audit effort has tended to remain stable year on year and sits in a similar range to coverage, yet proportionality ranks notably lower—suggesting audit responses may not be keeping pace with shifting workforce and capability needs.

By contrast, several long established audit areas display the opposite profile.

Financial risk ranks relatively lower for risk and severity, yet it is first for maturity and first for coverage and proportionality—signalling strong organisational capability and high audit confidence. That strength is positive, but it also prompts a discipline question: is the level of coverage still justified by current risk signals and stakeholder need, or is it sustained by familiarity? A similar, though less pronounced, pattern is evident for governance/reporting and fraud.

Climate and organisational culture sit mid table for risk ranking but remain comparatively weaker on maturity and internal audit coverage measures, indicating areas where assurance approaches may still be developing and where plans may need clearer statements of what "adequate" looks like.

BACK NEXT CONTENTS

INTERPRETING THE RESULTS: BLIND SPOTS, ANCHORS AND WHAT "ALIGNMENT" REALLY MEANS

10 Questions Chief Audit Executives should ask themselves

1. Where are the biggest gaps between risk ranking/ severity and our internal audit effort, coverage adequacy and proportionality—and are these conscious trade offs agreed with the Audit Committee?
2. Which risks in our plan look like "macro" (high importance/severity but low effort/coverage/ proportionality), and how have we translated them into auditable topics (strategy, resilience, supply chain, treasury, pricing, sanctions, business continuity)?
3. Which risks look like "digital disruption/AI" (high importance/severity, low maturity), and are we auditing the capability build (governance, accountability, controls, model risk, data quality, third parties, ethics and performance) rather than only project delivery or IT controls?
4. Do we have explicit criteria for when a risk "moves tier", and an agreed mechanism to reallocate resources quickly when external conditions change (mid year as well as annually)?
5. Where severity and uncertainty are high, are we providing assurance that tests decision making, resilience and preparedness (including scenario analysis and stress testing), not just compliance and control design?
6. Which areas resemble "financial" (strong maturity and high audit confidence despite lower risk ranking), and what could we stop or reduce to rebalance coverage toward fast rising risks?
7. Are our strongest coverage areas (financial, governance, fraud) still proportionate—supported by current risk signals, control dependence, regulatory expectation or incident trends—or are they anchored in historic practice?
8. Where internal audit effort and risk ranking appear aligned (for example, cybersecurity), have we tested whether the alignment is truly risk driven, or influenced by regulatory pressure, Audit Committee expectation or insufficient reliance on second line functions?
9. Have we agreed with stakeholders what "coverage" means for complex, cross cutting risks (AI, macro uncertainty), where assurance may need to be broader than a single audit?
10. Where we are increasing coverage (especially in AI), what success measures will demonstrate improved assurance outcomes (not simply more activity), and how will we report this to the Audit Committee?

FINDINGS
RISK RANKING

Cybersecurity and data security remains the dominant risk.

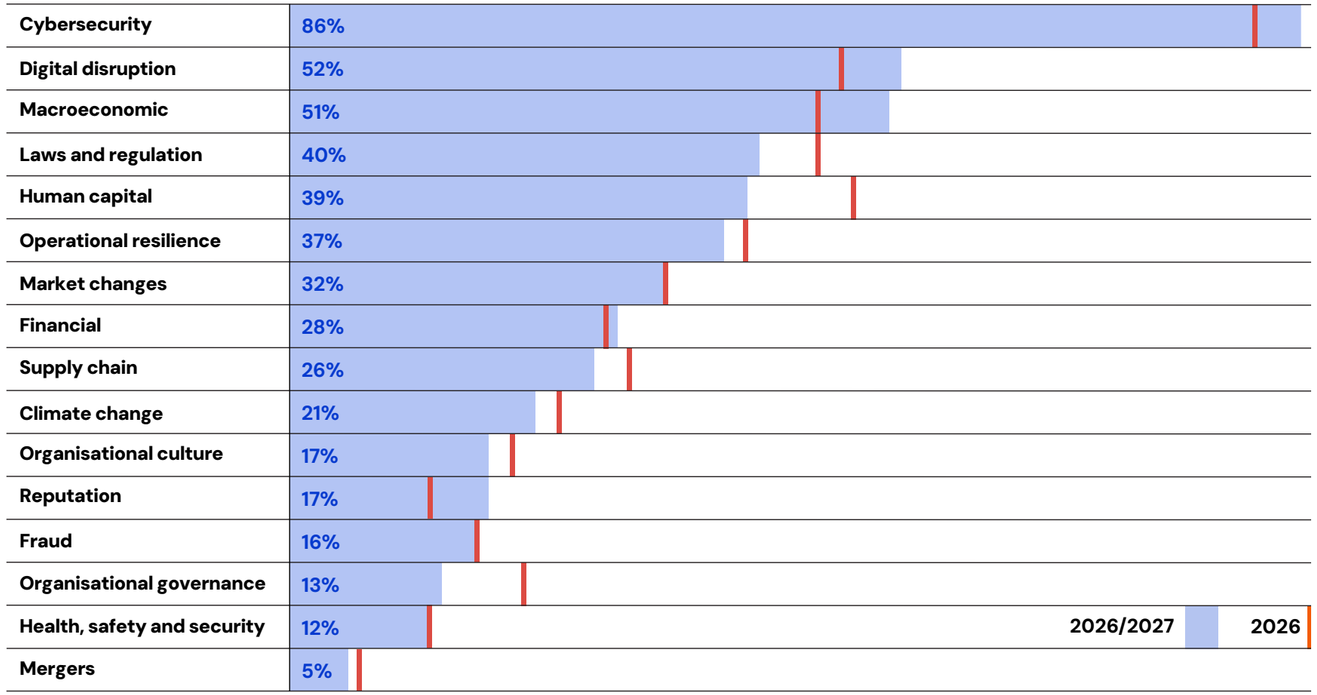
The "second tier" is now led by two risks that sit at roughly half of respondents:

- Digital disruption / new technologies / AI
- Macroeconomic, social and geopolitical uncertainty

Human capital, diversity, talent management and retention shows the largest decline in the top risk metric, falling from 2nd to 5th place.

New and changing laws and regulations has decreased in perceived importance.

The data indicates a shift towards disruption and uncertainty risks that are harder to "audit with a checklist" and often require internal audit to reassess its approach, coverage model, and skill mix.



Questions internal auditors should ask

1. Does our audit plan show a clear response to the rise in macro/geopolitical uncertainty and digital disruption/AI, or does it still reflect last year's priorities?
2. Where cyber is consistently top, do we have a plan that tests outcomes and resilience, not just controls and compliance?
3. Have we reduced our perception of the importance of human capital and regulation because risk has reduced, or because attention has been crowded out by cyber and uncertainty?
4. Do we have explicit criteria for when a risk "moves tier", and how quickly internal audit should re allocate coverage when it does?

FINDINGS
RISK SEVERITY

This is a new question in the survey this year and it showed some interesting results when compared to risk rankings.

Survey participants were asked to rank the severity of each risk on a scale of 1 -7, with 1 being very low and 7 being very high.

We see that the severity of the top three ranked risks is mirrored in their significance (Cybersecurity, Digital disruption and macroeconomic).

However, we also see operational resilience that is not ranked in the top 5, but the severity is significant enough to pull it into a top 5 severity position. This may be because operational resilience and particularly crisis management are tightly linked to the response of an organisation when the top three risks materialise.

Lower in the rankings, we also see two risks where the severity ranking is a lower position: financial and climate.

Cybersecurity	6.12
Digital disruption	5.28
Macroeconomic	5.12
Operational resilience	4.88
Laws and regulation	4.71
Human capital	4.7
Market changes	4.37
Supply chain	4.33
Organisational culture	4.14
Reputation	4.05
Financial	4.04
Organisational governance	3.87
Fraud	3.84
Climate change	3.66
Health, safety and security	3.58
Mergers	2.8

Questions internal auditors should ask

1. Where severity is high (cyber, disruption, macro), do we have audits that test decision-making, resilience and preparedness, not only technical controls?
2. Have we agreed with the audit committee what “severe” means in our context and how that triggers audit response?
3. Are we using scenario analysis or stress testing approaches in audit work where severity is high but uncertainty is also high?

FINDINGS
RISK MATURITY

Again, this is a new question introduced this year. It was introduced to enable the analysis to consider risk maturity, (i.e. the level of sustainable, repeatable and mature enterprise risk management) for each of the 16 risks that they have assessed for importance and severity in their organisation.

Participants were asked to rank the maturity of each risk with 1 being initial, 2 being infrastructure, 3 being integrated, 4 being managed and 5 being Level 5 optimised.

Digital disruption and macroeconomic risks were 2 and 3rd respectively for ranking and severity of risk. The risk maturity of both were the lowest according to the survey results in 16th and 15th place respectively. This suggests that the risk management capabilities are lagging behind the severity of the risks and therefore internal audit may need to adopt more advisory, capability building and governance focused approaches, not only assurance.

Average risk maturity scores were in the range of 2.87 to 4.16, implying many organisations see themselves as “developing” rather than immature or optimised.

An interesting result was the level of ‘Don’t know’ for mergers and acquisitions (19.7%) – ranked the lowest and with a severity of only 2.8, which may call into question the ranking and severity results if maturity is not known.

Financial, liquidity and insolvency has the highest maturity average (4.16), a clear distance from the next tier of Cybersecurity and Health & Safety.

Financial	4.16
Cybersecurity	3.67
Health, safety and security	3.66
Organisational governance	3.56
Reputation	3.56
Mergers	3.55
Laws and regulation	3.51
Market changes	3.41
Operational resilience	3.37
Supply chain	3.36
Fraud	3.34
Human capital	3.23
Organisational culture	3.16
Climate change	3.13
Macroeconomic	3.11
Digital disruption	2.87

Questions internal auditors should ask

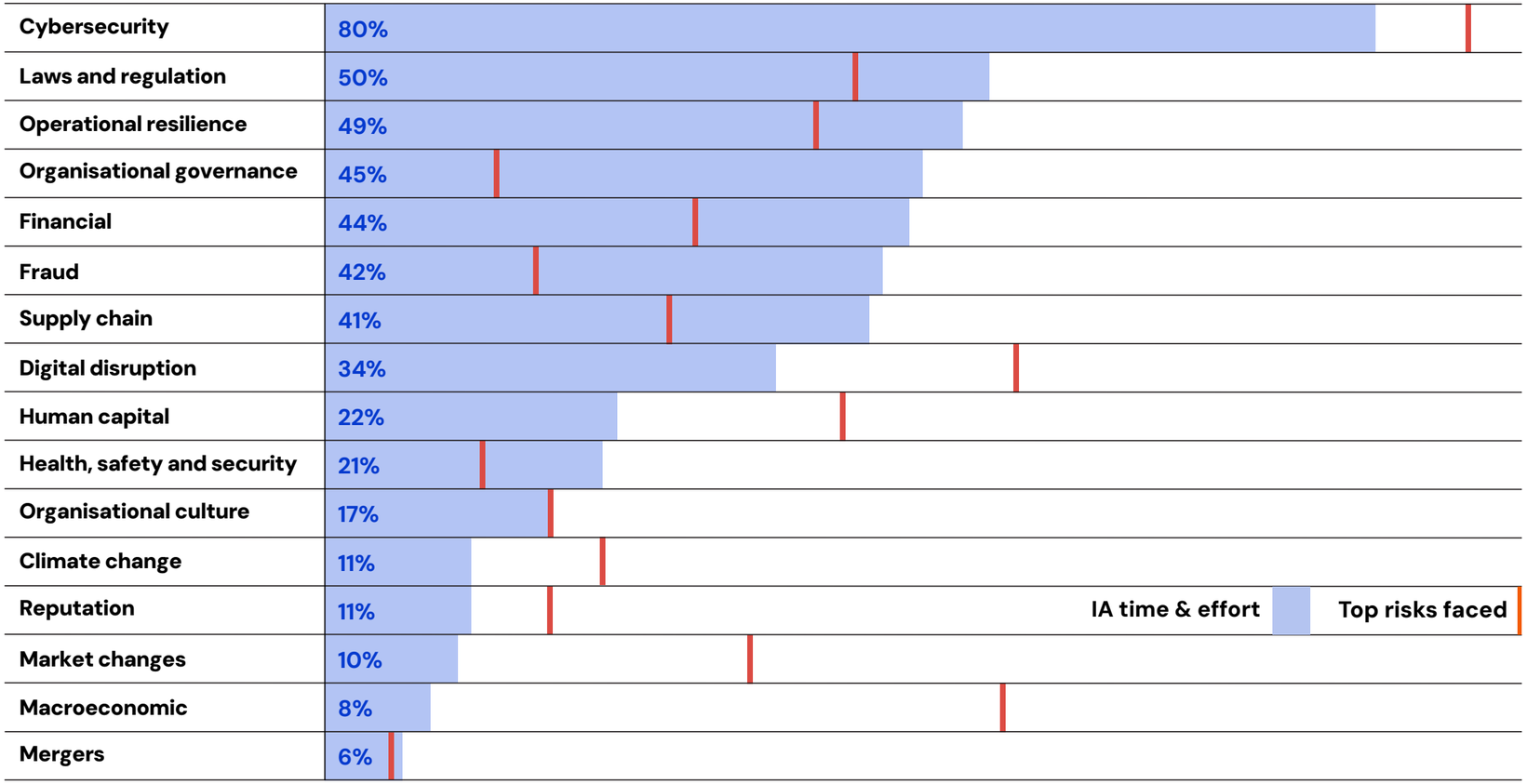
1. Where maturity is low (especially digital disruption/AI), have we defined what “good” looks like and how we will audit progress?
2. Do we have enough specialist support to credibly assess maturity in low maturity areas (for example, AI governance and transformation controls)?
3. Are we comfortable taking assurance over risks where management capability is still emerging, or do we need to adjust our assurance model?
4. Where maturity appears higher (financial), are we over auditing because it is familiar, rather than because risk is changing?

← BACK NEXT → CONTENTS

FINDINGS

IA EFFORT COMPARED TO RISK

Cybersecurity is the only area with absolute alignment of the risk ranking and internal audit time and effort – both being first place



The largest misalignment is macroeconomic/geopolitical uncertainty, which is ranked 3rd, but has the second-lowest amount of internal audit time and effort. Digital disruption/AI also has a misalignment, but not as severe as macroeconomic risk. This is likely because both are volatile risks which are largely driven by external factors. However, auditing of other linked risks, such as organisational resilience, supply chain and governance are likely to be providing assurance in these risk areas.

Several traditional areas show the opposite pattern, with IA effort higher than the risk, most notably governance/reporting and fraud.

The reasons for the misalignments for the two risks, aren't clear from the survey alone. This is something every IAF needs exploring. However factors such as the risk being driven externally, the volatility of risks, risk maturity of the organisation and the capabilities and mandated role of the internal audit function can all have a part to play.

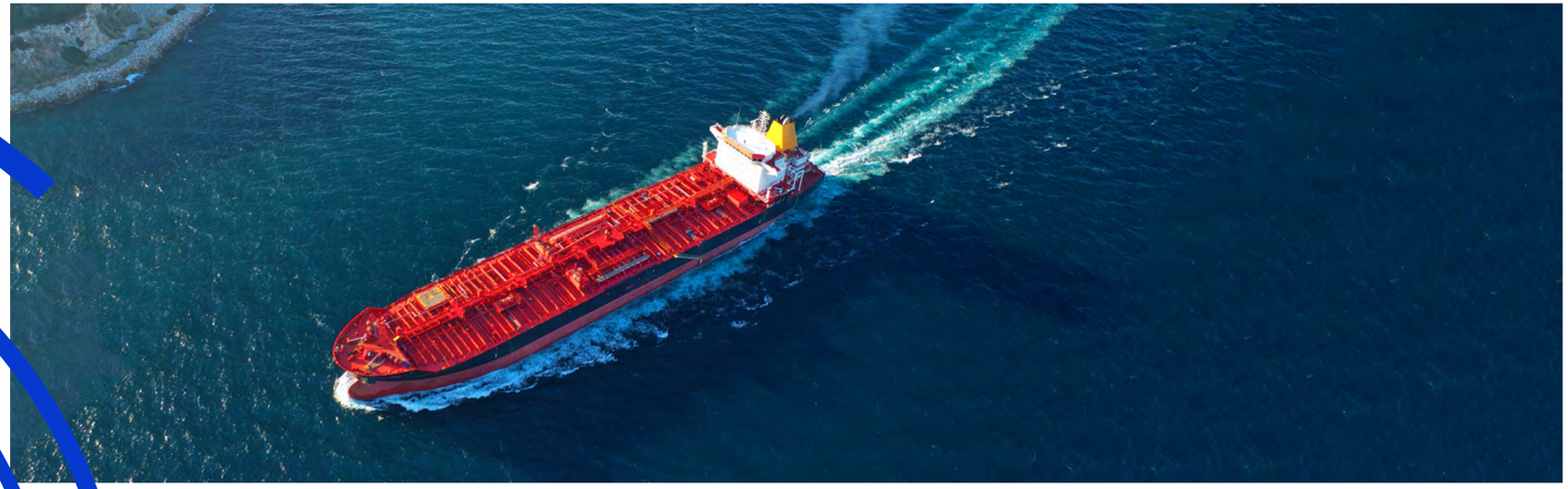
← BACK NEXT → CONTENTS

FINDINGS

IA EFFORT COMPARED TO RISK

Questions internal auditors should ask

1. Do we have an explicit planning mechanism that reallocates effort when a risk increases by this magnitude (for example, macro/geopolitical and AI)?
2. Are we under auditing macro/geopolitical risk because it is “outside the organisation”, or because we have not translated it into auditable topics (strategy, resilience, supply chain, treasury, pricing)?
3. Where IA effort is high relative to top risk perception (governance, fraud), is the coverage still justified by control dependence, regulatory expectation, or incident trends?
4. Does our plan demonstrate a clear link between risk identification and resource allocation, or are we driven mainly by the prior year plan?
5. Have we agreed with stakeholders what “coverage” means in complex risks like AI and macro uncertainty, where assurance may need to be broader than a single audit?
6. Where internal audit effort and risk ranking are aligned, as with cybersecurity, have we tested whether that alignment is risk-driven, or whether it reflects regulatory pressure, audit committee expectation or insufficient reliance on second line functions?



FINDINGS
IA COVERAGE ADEQUACY

This is a new question this year and is aimed at understanding CAE's perceptions as to whether the IA coverage is at the right level for each risk

Participants were asked to score the internal audit coverage adequacy of each risk, with 1 being inadequate coverage and 7 being full and adequate coverage.

Adequacy is rated highest in more established domains: financial and governance/reporting. Cyber and fraud also score strongly, in the next tier.

The lowest adequacy scores include high risk ranked areas such as digital disruption, macroeconomic and human capital – indicating that CAEs feel that the audit plans are not providing the assurance level needed for these areas.

Financial	5.04
Organisational governance	5.01
Cybersecurity	4.9
Fraud	4.89
Operational resilience	4.83
Laws and regulation	4.8
Supply chain	4.47
Health, safety and security	4.28
Organisational culture	4.1
Reputation	4.07
Human capital	3.91
Digital disruption	3.83
Climate change	3.62
Market changes	3.44
Macroeconomic	3.28
Mergers	3.19

Questions internal auditors should ask

1. Which of the lowest adequacy areas are most relevant to our organisation, and what would "adequate coverage" look like in practice?
2. Are we providing enough coverage of climate/sustainability and market change, or have we treated these as secondary compared to other risks, such as cyber?
3. For AI and digital disruption, are we auditing the right things (governance, model risk, data quality, third parties, ethics, performance), or only project delivery and IT controls?
4. Have we discussed these perceived adequacy gaps explicitly with the audit committee and agreed how they will be addressed in the annual plan?
5. Is coverage inadequacy driven by IAF internal factors (insufficient resources / audit universe focus / misalignment with 2nd line activities / lack of dynamic planning); organisation factors (low risk management maturity) or IAF external factors (coverage mandated by the board, regulator, other involved parties).

← BACK NEXT → CONTENTS

FINDINGS
IA PLAN PROPORTIONALITY

Another new question this year to ask CAEs if they think that the audit plan coverage is proportionate to the risk. This goes beyond "are internal audit covering it?" and asks "is the balance right?". It is a direct challenge to the credibility of the plan as risks shift.

Survey participants were asked how confident they were that internal audit coverage across risk areas was proportionate to the risks their organisation was facing, with 1 being not confident through to 7 being very confident.

The proportionality scores are in a tight range of 4.04 and 5.37 – firmly in the upper middle of the 1-7 scoring available. This suggests that CAEs are highly satisfied with the time spent, even though for a number of risks the time spent substantially appears to lag behind the level of the risks.

Proportionality scores are strongest in traditional areas such as financial governance/ reporting and fraud. The lowest proportionality scores, but still above the average of 4, appear in:

- Macro/geopolitical uncertainty.
- Digital disruption/AI.
- Market changes.

There are some similarities here with the previous question on coverage, meaning that the IA's coverage is based in risk assessment – to an extent.

Financial	5.37
Organisational governance	5.13
Fraud	5.04
Laws and regulation	5.03
Operational resilience	4.9
Health, safety and security	4.84
Cybersecurity	4.83
Climate change	4.72
Supply chain	4.7
Reputation	4.55
Organisational culture	4.46
Human capital	4.37
Mergers	4.33
Market changes	4.22
Digital disruption	4.11
Macroeconomic	4.04

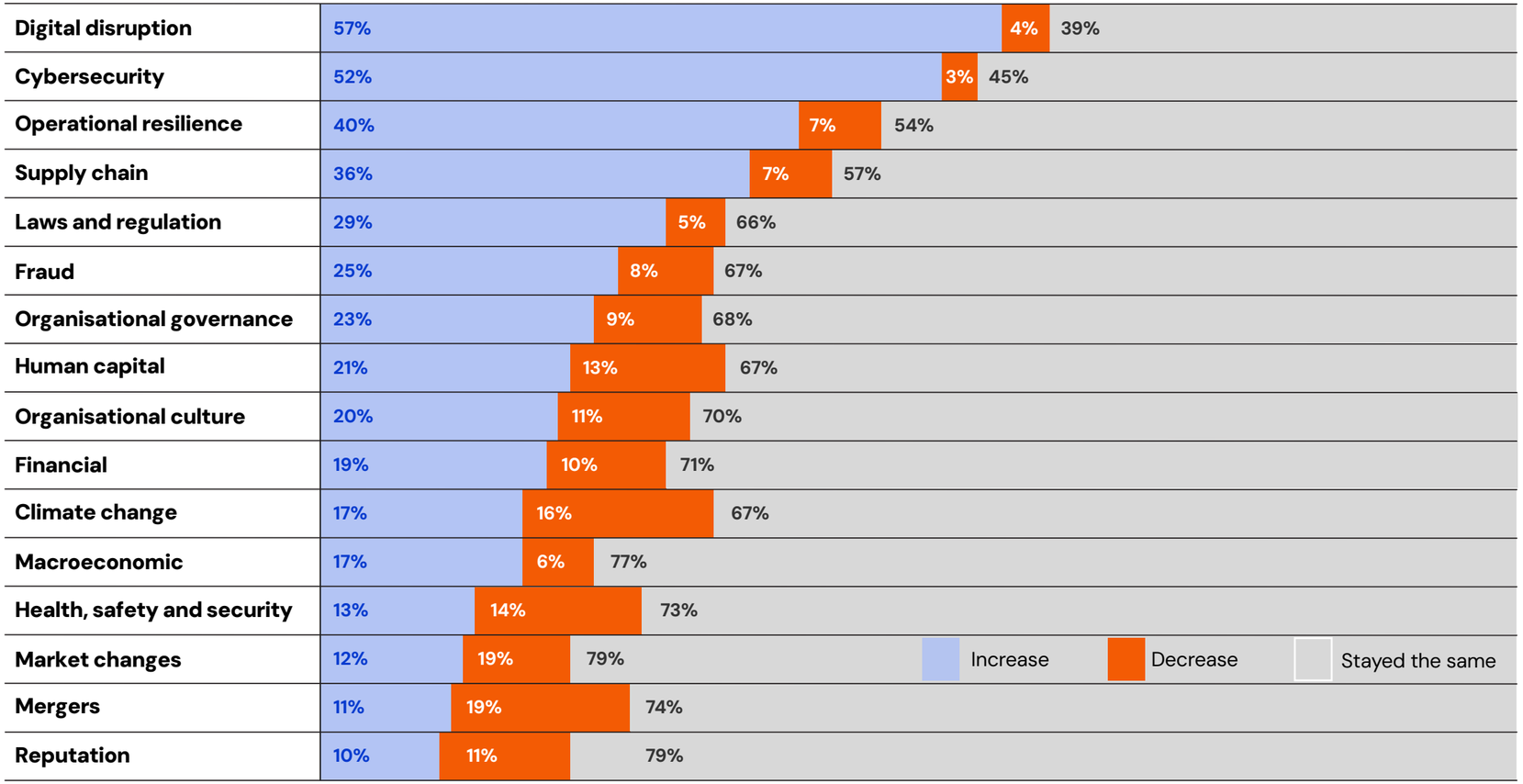
Questions internal auditors should ask

1. Are we being too positive about the proportionality of the time spent on the real high risks for the organisation?
2. If our proportionality is weaker in macroeconomics and AI, is this because we are under auditing those risks, or because we are over auditing other areas?
3. What evidence do we use to justify proportionality: risk appetite, incidents, assurance mapping, investment levels, regulatory requirements, or audit committee/board expectations?
4. Are we confident our assessment of the audit universe captures the ways macro/geopolitical risk manifests, such as treasury, supply chain, sanctions, pricing, capital allocation, and business continuity?
5. Do we regularly re validate proportionality mid year when external conditions change, or only annually?

FINDINGS

CHANGES IN IA PLAN COVERAGE

In previous years we have asked CAEs to predict 3 years into the future, however with the volatile landscape and increased pace of change, this was not adding value. So this new question was introduced to compare the previous year with the next.



The biggest reported increases in IA coverage are in: Digital disruption/AI, Cybersecurity, Operational resilience and Supply chain. A notable decrease manifests for climate change/biodiversity/sustainability - a pattern already indicated in our last year's report.

"Stayed the same" is the largest response for all but the top two ranked risks, suggesting coverage change is incremental rather than transformational.

Some areas show higher "decrease" signals than others (for example, M&A and climate have notable decrease proportions), which may reflect strategic reprioritisation or resource constraint. It also reflects the risk ranking reduction over the past 2 years of climate change and M&A consistently being the lowest ranked risk.

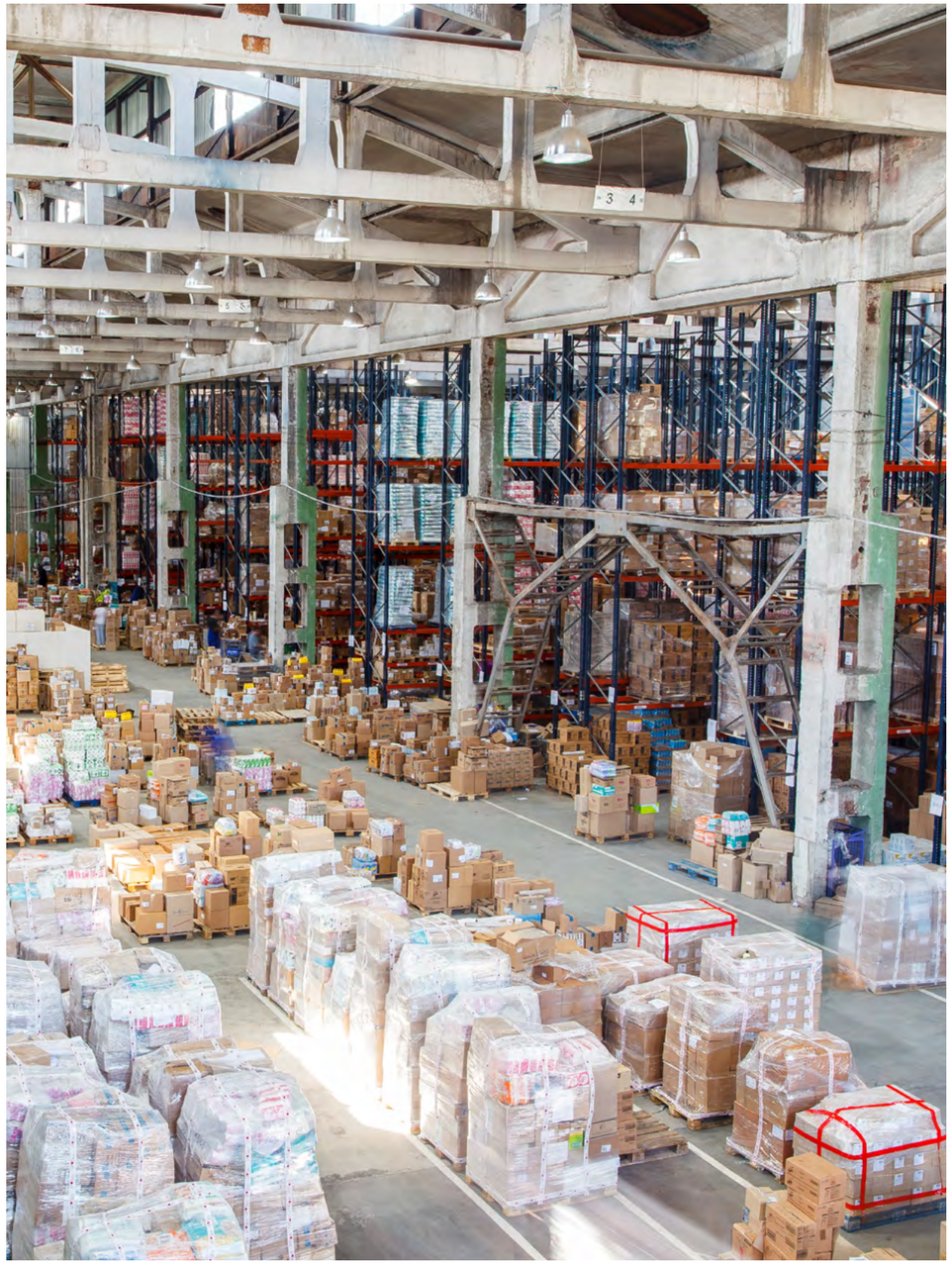
Internal audit is moving in the direction of significantly increasing coverage of cybersecurity and disruption, but the extent of change may not yet match the scale of risk movement, particularly where capability is low and assurance approaches are emerging.

BACK NEXT CONTENTS

FINDINGS
CHANGES IN IA PLAN COVERAGE

Questions internal auditors should ask

1. Where we have increased coverage, did we increase the right type of coverage (assurance vs advisory, controls vs governance, point audits vs continuous monitoring)?
2. Have we increased coverage because the risk rose, or because regulators, boards, or incidents demanded it?
3. Where coverage stayed the same, what prevented change: lack of skills, lack of mandate, crowded plan, or uncertainty about how to audit the topic?
4. Are we confident we can sustain increased focus in cyber and AI without creating blind spots elsewhere?
5. Do we track whether changes in coverage actually improve assurance outcomes, or do we measure change only by time allocation?



BACK NEXT CONTENTS

CONCLUSION

This interim report reinforces a simple conclusion: the credibility of internal audit is increasingly defined by how quickly and confidently it can realign assurance as risks evolve. In a landscape shaped by volatility, rapid technological change and growing interconnection between risks, annual planning cycles and familiar coverage patterns can lag the reality faced by boards and executive teams.

For Chief Audit Executives, the practical challenge is not whether every emerging risk is "covered", but whether the assurance model is fit for purpose—testing outcomes, resilience and decision making where risks are strategic, externally driven or still maturing. That requires more explicit choices about what to deepen, what to stop, and how to evidence that resources are being deployed in line with today's risk signals rather than yesterday's audit universe.

The findings also underline the value of clarity: agreeing with stakeholders what "adequate" and "proportionate" coverage mean for complex, cross cutting risks; making regulatory drivers visible even when they sit within broader categories; and defining success measures when coverage is increased so progress is demonstrated through better assurance outcomes, not simply more activity. Where specialist capability is required, CAEs may need to invest differently—through skills, co sourcing or new assurance techniques—to maintain confidence in judgements about risk and control effectiveness.

Ultimately, Risk in Focus 2026/27 is a prompt for deliberate rebalancing. Audit functions will be judged less on the breadth of their checklist and more on the quality of their insight—how well they anticipate change, surface trade offs, and help the Audit Committee take comfort that assurance remains aligned to the risks that matter most.

APPENDIX I - METHODOLOGY

The findings in this report are based on a UK & European survey of Chief Audit Executives (CAEs). The survey was open from 2 March to 7 April and attracted 797 completed responses from across Europe. Responses covered a broad mix of countries, sectors and organisation sizes.

Respondents were asked to assess the following:

- The top risks facing their organisation
- The severity of those risks
- The maturity of their organisation's risk management in each area
- The time and effort internal audit devotes to each area
- The adequacy and proportionality of current audit coverage
- Whether internal audit coverage has increased, decreased or remained stable over time

APPENDIX II - RISK CATEGORIES

1. Climate change, biodiversity and environmental sustainability	Climate impacts, resource scarcity, biodiversity loss and tightening environmental regulations affecting operations and strategy.
2. Cybersecurity and data security	Cyberattacks, ransomware, data breaches and identity compromise undermining digital security and trust.
3. Digital disruption, new technologies and AI	Rapid technological change, AI adoption risks, system failures and technology driven market disruption.
4. Financial, liquidity and insolvency	Macroeconomic volatility, inflation, market instability and cash flow pressures heightening insolvency risk.
5. Fraud, bribery and criminal exploitation of disruption	Fraud, corruption, financial crime and opportunistic exploitation during periods of instability or crisis.
6. Health, safety and security	Physical harm, security threats, well-being risks and unsafe operating conditions, including geopolitical instability.
7. Human capital, diversity, talent management and retention	Labour market shortages, demographic trends, skills gaps and evolving cultural expectations affecting workforce stability.
8. Macroeconomic, social and geopolitical uncertainty	Political conflict, sanctions, social unrest and global economic shocks influencing organisational exposure.
9. Market changes, competition and evolving consumer behaviour	Shifting customer demand, competitive disruption, innovation cycles and rapid market transformation.
10. Mergers and acquisitions	Financial transaction and legal risks, valuation uncertainty, integration challenges and post deal instability impacting performance.
11. New and changing laws and regulations	New or evolving legal requirements, regulatory expectations or jurisdictional divergence are creating compliance pressure.
12. Operational resilience, crisis management, business continuity and disaster response	Disruptive shocks such as cyberattacks, natural hazards, supply chain failures or infrastructure outages affecting operational stability.
13. Organisational culture	Misconduct, leadership failures, poor behaviour and cultural resistance creating organisational vulnerability.
14. Organisational governance and corporate reporting	Governance failures, ethical breaches, reporting inaccuracies and rising transparency expectations.
15. Reputation, communication and stakeholder relationship	Public criticism, media pressure, misinformation or regulatory scrutiny that damages trust and organisational reputation.
16. Supply chain, outsourcing and nth party risk	Supplier failures, geopolitical constraints, logistics disruption and weaknesses across extended third party ecosystems.

APPENDIX III - SURVEY QUESTIONS

1. Please select and rank the top 5 risks your organisation is currently facing (1st being the biggest risk)
2. Please rate the severity of the following risks for your organisation in 2026/27.
3. For each risk category, please rate the level of risk maturity at your organisation.
    - Level 1 – Initial, e.g. ad hoc and unstructured governance
    - Level 2 – Infrastructure, e.g. has structures in place, but not much beyond the mechanics of a process
    - Level 3 – Integrated, e.g. co-ordinated across the organisation with good interaction
    - Level 4 – Managed, e.g. Very good reporting and use of dashboards for risk-based decision making
    - Level 5 – Optimised, e.g. Fully embedded and transparent with excellent professionally challenging discussions and variety of views fully explored before decisions are made for the benefit of the organisation.
    - Don't know
4. Please rank the top 5 risk areas on which internal audit currently spends the most time and effort (1st being the risk where most time is spent)
5. How would you rate the adequacy of internal audit's current coverage across the following risk areas? (1 being inadequate coverage and 7 being full and adequate coverage.)
6. How confident are you that internal audit coverage across the listed risk areas is proportionate to the risks your organisation is facing? (1 being not confident, 7 being very confident.)
7. In comparison to your 25/26 internal audit plan has your 26/27 internal audit plan coverage increased, decreased or stayed the same?

ABOUT RISK IN FOCUS

For the past 11 years, Risk in Focus has highlighted key risk areas to help internal auditors prepare for independent risk assessment work, annual planning and audit scoping. It helps Chief Audit Executives (CAEs) understand how their peers view today's risk landscape as they prepare their audit plans for the year ahead.

This year, Risk in Focus 2026/2027 involved collaboration between 13 European Institutes of Internal Auditors, spanning 14 countries: Austria, Belgium, France, Germany, Greece, Hungary, Ireland, Italy, the Netherlands, Norway, Spain, Sweden, Switzerland and the UK.

The survey received 797 responses from CAEs across Europe.

IIA Austria

Institute of Internal Auditors Belgium

IFACI Elevating Impact

DIIR Deutsches Institut für Interne Revision e.V.

Institute of Internal Auditors Greece

The Institute of Internal Auditors Hungary

Associazione Italiana Internal Auditors

The Institute of Internal Auditors Netherlands

The Institute of Internal Auditors Norway

Instituto de Auditores Internos de España

IIA Sweden

The Institute of Internal Auditors Switzerland

Chartered Institute of Internal Auditors

ECIIA