GLOBAL SUMMARY 2026/2027

Hot Topics for Internal Auditors

RISK in FOCUS

Internal Audit
FOUNDATION
1976-2026

ABOUT GLOBAL RISK IN FOCUS

Know Your Risks. Plan Strategically.

Risk in Focus is the Internal Audit Foundation's premier annual initiative to identify the five most significant risks impacting the world.

Learn what internal auditors are saying about the:

- Five highest risks in their region
- Five top priorities for internal audit effort
- Key considerations for boards and audit committees

Risk in Focus uses survey results, regional roundtables, and interviews with local experts to reveal key insights from the unique perspective of internal auditing.

The Internal Audit Foundation gratefully acknowledges the work of IIA National Institutes and IIA regional bodies that make this research possible: African Federation of Institutes of Internal Auditors (AFIIA), Arab Confederation of Internal Auditors (ARABCIA), Asian Confederation of Institutes of Internal Auditors (ACIIA), European Confederation of Institutes of Internal Auditors (ECIIA), and Fundación Latinoamericana de Auditores Internos (FLAI).

Special appreciation goes to the European Institutes Research Group (EIRG), which developed the Risk in Focus research approach in 2016 and continues to publish the report for Europe through the ECIIA.

All reports and board briefings are free to the public:

- Africa
- Asia Pacific
- Europe
- Latin America
- Middle East
- North America
- Global Summary

Visit the Risk in Focus Knowledge Center to learn more.

50 Internal Audit FOUNDATION 1976-2026

Visit the Risk in Focus Knowledge Center for free reports and board briefings (theiia.org/RiskInFocus).

GLOBAL RESEARCH PARTICIPATION

132 countries/ territories

3,285 survey responses

17 roundtables with **149** participants

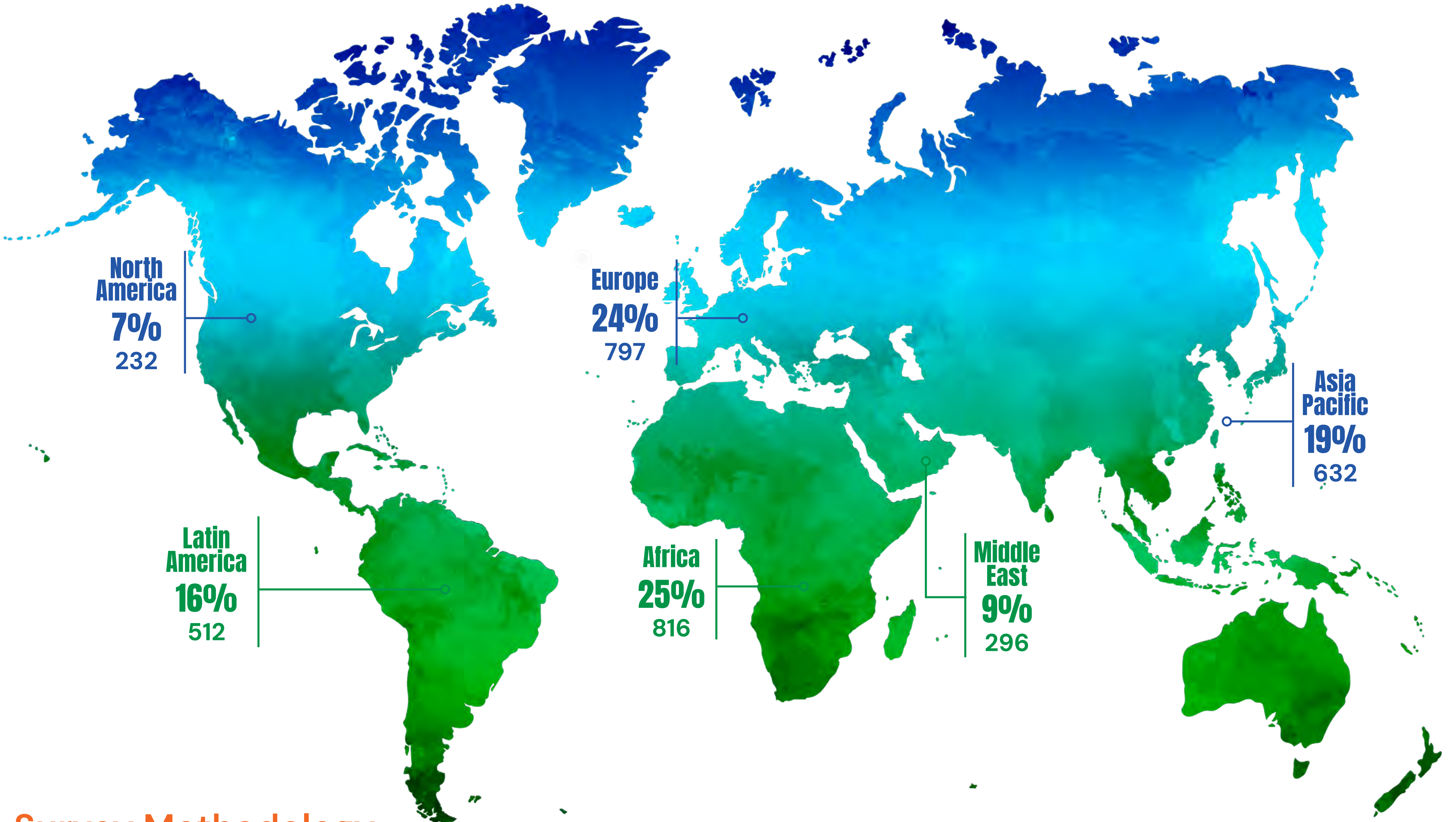
12 in-depth interviews

GLOBAL SURVEY PARTICIPATION

GLOBAL TOTALS

3,285 respondents

132 countries/locations



Survey Methodology

Survey responses were received from 3,285 chief audit executives and directors representing 132 countries and locations. The Internal Audit Foundation hosted the survey online from March 24 to May 6, 2026, for all regions except Europe. The survey for Europe was conducted by the European Institutes Research Group from March 2 to April 7, 2026.

CONTENTS

EXECUTIVE SUMMARY

From Risk Rankings to Adaptive Assurance

The global risk environment is not being reshaped by one dominant threat, but by the convergence of rapidly rising risks related to cybersecurity, digital disruption, and geopolitical uncertainty. For chief audit executives, the central challenge is no longer identifying change. It is translating rapid and interconnected change into timely assurance, practical advice, appropriate capabilities, and decisions by boards and senior management.

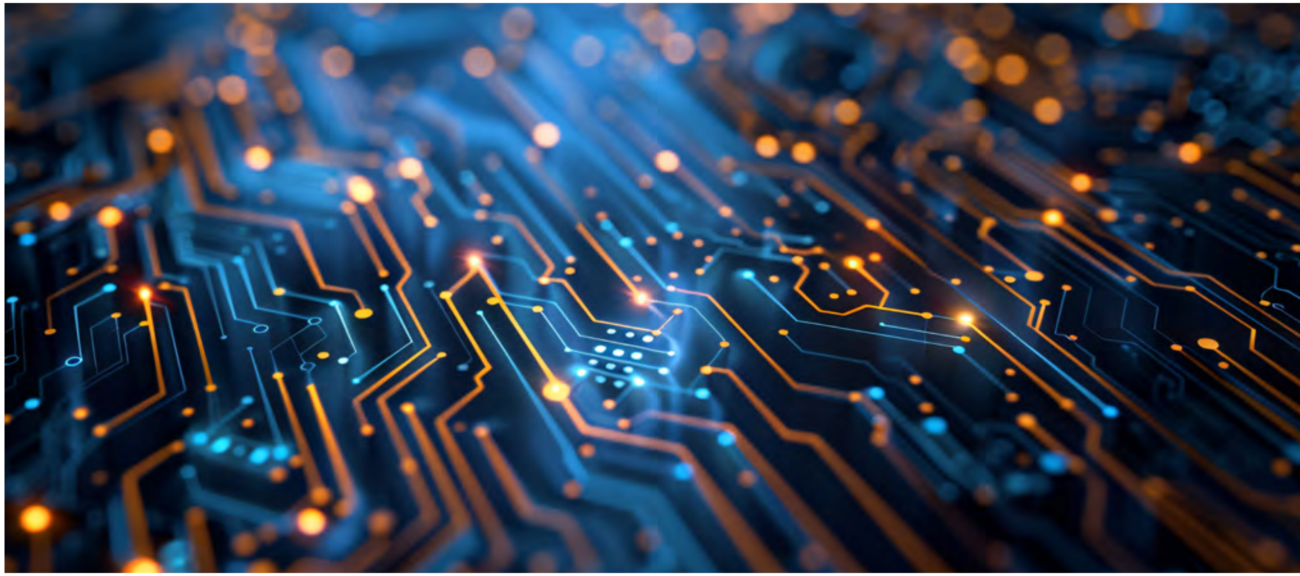
The 2026/2027 Risk in Focus findings, based on responses from 3,285 chief audit executives and directors in 132 countries and locations, reveal a risk environment that is becoming more digital, volatile, and interconnected. Global risks converged into three areas:

- **Cybersecurity** remains the world's dominant risk, chosen by 80% of respondents as one of their five highest risks (Exhibit 1.1).
- **Digital disruption,** including artificial intelligence, ranks second at 58% and rose 10 percentage points over the prior year (Exhibit 1.1).
- **Geopolitical/macroeconomic uncertainty** also increased 10 percentage points, reaching 48% (Exhibit 1.1).

Not only were these three risks the highest worldwide, but their risk levels also increased for nearly every region within the past year. This risk convergence occurred as organizations worldwide experienced common pressures, creating a shared risk environment with global implications.

In roundtables around the world, internal audit leaders discussed the implications of the current risk environment, with five themes emerging:

- **Technology and geopolitical risks are becoming systemic.** Cybersecurity, AI, conflict, trade policy, regulatory change, energy constraints, and third-party dependencies can affect strategy, operations, liquidity, fraud, reputation, and resilience simultaneously.



EXECUTIVE SUMMARY

- **Risk displacement occurs as urgent, disruptive risks push other risks out of the Top 5 risk ranking.** However, the displaced risks can still have high risk severity. For example, business resilience dropped to 35% in the Top 5 rankings, but 56% of survey respondents still consider the risk severity to be high. Similarly, regulatory change dropped to 32% in the Top 5 ranking, but 48% still rated the risk severity as high (Exhibits 1.1 and 1.3).

- **Internal audit effort is shifting toward high risk areas, but key gaps remain between risk level and audit priority.** The largest increase in audit priority was for digital disruption. Even with this change, a much higher percentage said digital disruption was one of their Top 5 risks (58%) compared to Top 5 audit priority (42%). Similarly human capital and geopolitical uncertainty had high risk ratings compared to their audit priority levels (Exhibits 1.1 and 2.1).

- **Audit plans retain strong traditional anchors.** Financial/liquidity, fraud, governance/corporate reporting, business resilience, and regulatory change receive greater audit priority compared to their Top 5 risk rankings. Much of this coverage is necessary, but it can reduce the capacity available for emerging and externally driven risks (Exhibit 2.1).

- **The most rapidly changing risks have some of the weakest governance and coverage.** Only 23% rated digital disruption governance as managed or optimized, and only 11% considered internal audit coverage fully adequate. For geopolitical/macroeconomic uncertainty, the equivalent results were 29% and 10% (Exhibit 3.1).

Regional differences remain important (Exhibit 1.2). Africa reports heightened fraud and financial pressure; Asia Pacific emphasizes digital disruption, supply chains, resilience, and talent; Europe faces elevated cyber, geopolitical, and regulatory risk; Latin America highlights cyber, AI, geopolitics, and fraud; the Middle East demonstrates how conflict can rapidly transform resilience and liquidity; and North America reports the highest digital disruption risk.

The mandate for CAEs is clear: develop dynamic plans, assess risks as connected systems, compare risk with maturity and coverage, coordinate assurance across the Three Lines, and build the capabilities needed to address what the organization is becoming — not only what it has historically been.

Risk displacement occurs as urgent, disruptive risks push other risks lower in the risk rankings.

BACK NEXT CONTENTS

1. GLOBAL RISK ENVIRONMENT

Three Accelerating Risks, One Interconnected System

Cybersecurity, digital disruption, and geopolitical/macroeconomic uncertainty form the core of the global risk environment. Their significance goes beyond their individual rankings. Each can transmit risk across organizational boundaries and convert quickly into operational disruption, financial loss, fraud, regulatory exposure, reputational damage, or a crisis of stakeholder confidence.

Cybersecurity becomes an enterprise risk

Cybersecurity remains the highest global risk, rising seven percentage points to 80% (Exhibit 1.1). It increased in every region except North America, where it was already exceptionally high at 85% (Exhibits 1.2).

The attack surface now includes cloud platforms, software ecosystems, AI models, digital identities, remote access, operational technology, outsourced processes, data repositories, mobile applications, and interconnected third parties. AI can improve threat detection and response, but it can also enable more sophisticated phishing, synthetic identities, voice and image impersonation, automated exploitation, and fraud. AI is a key driver of cybersecurity risks.

The result is that cybersecurity cannot be treated only as a technical control domain. A cyber event may become a business interruption, fraud, privacy breach, regulatory violation, supply chain failure, safety event, or reputational crisis. Internal audit therefore needs to assess both preventive controls and the organization's ability to detect, respond, recover, communicate, and learn.

Digital disruption moves from future risk to present pressure

Digital disruption risk ratings rose 10 percentage points to 58%, with increases in every region. North America reported the highest level at 69%, followed by Latin America at 61%, Asia Pacific at 59%, the Middle East at 58%, Europe at 52%, and Africa at 50%. (Exhibits 1.1 and 1.2).

The regional drivers differ. In some organizations, digital disruption means moving from manual processes to digital operations. In others, it means integrating generative AI, autonomous agents, advanced analytics, robotics, cloud platforms, and AI-enabled products into already complex environments.

Yet a common pattern emerges — adoption often moves faster than governance. Organizations may deploy AI before they have established clear ownership, inventories, data standards, risk classification, approval requirements, human oversight, monitoring, incident escalation, or model validation.

Digital disruption also affects other risks. It changes workforce needs, fraud scenarios, third-party dependencies, regulatory obligations, competitive dynamics, customer expectations, and the economics of existing business models. CAEs should therefore assess AI and digital transformation as components of a broader risk network, not as isolated technology projects.

"Sometimes adoption is faster than the governance framework can evolve."

– CAE, Financial Services, Kuwait

Exhibit 1.1. Global – Top 5 Risks Trend

Survey question: **What are the Top 5 risks your organization currently faces? (Choose 5.)**

2023	2024	2025	2026	Change from 2025 to 2026	Change	Risk areas
73%	**71%**	**73%**	**80%**		**+7**	**Cybersecurity**
34%	**39%**	**48%**	**58%**		**+10**	**Digital disruption (including AI)**
30%	**28%**	**38%**	**48%**		**+10**	**Geopolitical/ macroeconomic uncertainty**
51%	49%	43%	38%		-5	Human capital
47%	54%	47%	35%		-12	**Business resilience**
32%	32%	31%	34%		+3	Financial/liquidity
39%	**37%**	**41%**	**32%**		-9	**Regulatory change**
32%	**32%**	**31%**	**29%**		-2	**Market changes/competition**
24%	**27%**	**23%**	**29%**		**+6**	**Fraud**
26%	22%	24%	27%		+3	Supply chain and outsourcing
27%	26%	24%	20%		-4	Governance/corporate reporting
19%	21%	18%	19%		+1	Climate change/environment
26%	25%	24%	19%		-5	Organizational culture
21%	21%	19%	15%		-4	Communications/reputation
11%	11%	10%	10%		0	Health/safety
6%	6%	5%	5%		0	Mergers/acquisitions

Increased risk compared to prior year   Decreased risk compared to prior year

How to Interpret the Graph
Orange text indicates an increase of 4 percentage points or more compared to the prior year. The orange and blue bars show the difference in ratings from 2025 to 2026. The column labeled "change" shows the percentage point difference from 2025 to 2026.

Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 3,285.

← BACK NEXT → CONTENTS

GLOBAL RISK ENVIRONMENT

Geopolitical uncertainty becomes operational

Geopolitical/macroeconomic uncertainty risk ratings increased 10 percentage points to 48%. This risk rose in every region except North America, where it remained elevated after a significant increase in the previous year (Exhibits 1.1 and 1.2).

The Middle East reported the highest rating at 60% (Exhibit 1.2), reflecting the effects of the conflict that started when the U.S. and Israel initiated a joint attack against Iran on February 28, 2026. This conflict has impacted the Middle East's trade, energy, tourism, liquidity, supply chains, infrastructure, and business continuity.

Organizations cannot control war, elections, sanctions, tariffs, diplomatic disputes, inflation, interest rates, or currency movements. However, they can evaluate and strengthen their preparedness for the consequences. Internal audit can assess scenario planning, liquidity stress testing, supply chain concentration, regulatory monitoring, market entry decisions, crisis governance, business continuity, energy dependency, cloud concentration, and third-party resilience.

This transformation from external risk to internal operations is essential. Geopolitical risk becomes auditable when it is connected to an organizational objective, dependency, decision, process, or response capability.

Regional differences require contextual judgment

As shown in Exhibit 1.2, the global averages conceal meaningful regional differences:

- In **Africa**, cybersecurity leads at 73%, while fraud and digital disruption are both 50%, and financial/liquidity reaches 49%. Technology adoption, cyber-enabled fraud, debt, skills gaps, and economic pressure reinforce one another.
- In **Asia Pacific**, cybersecurity reaches 72%, digital disruption 59%, geopolitical/macroeconomic uncertainty 48%, business resilience 43%, and human capital 41%. Supply chain risk is relatively high.
- In **Europe**, cybersecurity is highest among all regions at 86%. Digital disruption reaches 52%, geopolitical uncertainty 51%, and regulatory change 40%.
- In **Latin America**, cybersecurity reaches 80%, digital disruption 61%, geopolitical uncertainty 52%, fraud 38%, and human capital 37%.
- In the **Middle East**, cybersecurity reaches 81%, geopolitical uncertainty 60%, digital disruption 58%, business resilience 47%, and financial/liquidity 42%.
- In **North America**, cybersecurity reaches 85% and digital disruption 69%, followed by human capital at 45%, geopolitical uncertainty at 43%, regulatory change at 42%, and market changes at 41%.

Geopolitical risk becomes auditable when it is connected to an organizational objective, dependency, decision, process, or response capability.

← BACK NEXT → CONTENTS

Exhibit 1.2. Global – Top 5 Risks per Region

Survey question: **What are the Top 5 risks your organization currently faces? (Choose 5.)**

Risk areas	Average of the regions	Africa	Asia Pacific	Europe	Latin America	Middle East	North America
Cybersecurity	**80% ↑**	**73% ↑**	**72% ↑**	**86% ↑**	**80% ↑**	**81% ↑**	**85%**
Digital disruption (including AI)	**58% ↑**	**50% ↑**	**59% ↑**	**52% ↑**	**61% ↑**	**58% ↑**	**69% ↑**
Geopolitical/macroeconomic uncertainty	**48% ↑**	**35% ↑**	**48% ↑**	**51% ↑**	**52% ↑**	**60% ↑**	**43%**
Human capital	**38%**	30%	**41%**	**39%**	**37%**	34%	**45%**
Business resilience	**35%**	28%	**43%**	37%	25%	**47%**	29%
Financial/liquidity	34%	**49% ↑**	**28% ↑**	28%	**36% ↑**	**42% ↑**	24%
Regulatory change	32%	28%	24%	**40%**	36%	20%	**42%**
Market changes/competition	29%	20%	37%	32%	27%	20%	**41% ↑**
Fraud	29%	**50% ↑**	**28% ↑**	16%	**38% ↑**	22%	**18% ↑**
Supply chain and outsourcing	**27% ↑**	**21% ↑**	**33% ↑**	26%	17%	**35% ↑**	33%
Governance/corporate reporting	20%	27%	21%	13%	15%	27%	14%
Climate change/environment	19%	**31% ↑**	20%	21%	23%	15%	7%
Organizational culture	19%	26%	19%	17%	26%	13%	16%
Communications/reputation	15%	18%	13%	**17% ↑**	15%	13%	16%
Health/safety	10%	12%	8%	12%	7%	10%	11%
Mergers/acquisitions	5%	2%	6%	5%	4%	3%	7%

5 highest risks

How to Interpret the Graph
The **red arrows ↑** indicate an increase of 4 percentage points or more compared to the prior year.

Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 3,285.

GLOBAL RISK ENVIRONMENT

These variations demonstrate why global benchmarking should challenge — not replace — the organization's own risk assessment.

Risk ranking, risk severity, and risk displacement

Exhibit 1.3 provides an important complementary view of risk.

The Top 5 risk rating shows which risks survey respondents chose as one of the 5 highest risks facing their organizations. The risk severity rating captures which risk were assessed as high, very high, or extremely high on a scale of 1 to 7.

The distinction matters. A risk that is not selected as Top 5 may still be significant. Business resilience, for example, was selected by 35% as a Top 5 risk but rated as high by 56%. Market changes/competition was selected by 29%, while 53% rated it as high. Human capital was chosen by 38%, but 54% rated it as high.

These differences suggest risk displacement. Respondents must choose only five areas, so rapidly rising risks may push other significant risks down the ranking. CAEs should therefore avoid interpreting a falling Top 5 percentage as automatic evidence that exposure has declined. CAEs should present the board with both Top 5 rankings and high-risk severity ratings to reduce the risk of false comfort caused by ranking displacement.

Conclusion: From isolated risks to risk pathways

The most consequential events rarely remain within one category. AI adoption can create data, cyber, compliance, fraud, talent, third-party, and reputation risks. A geopolitical event can create supply disruption, price volatility, liquidity pressure, regulatory change, operational interruption, and social instability. A cyberattack can trigger financial loss, customer harm, regulatory action, and loss of trust.

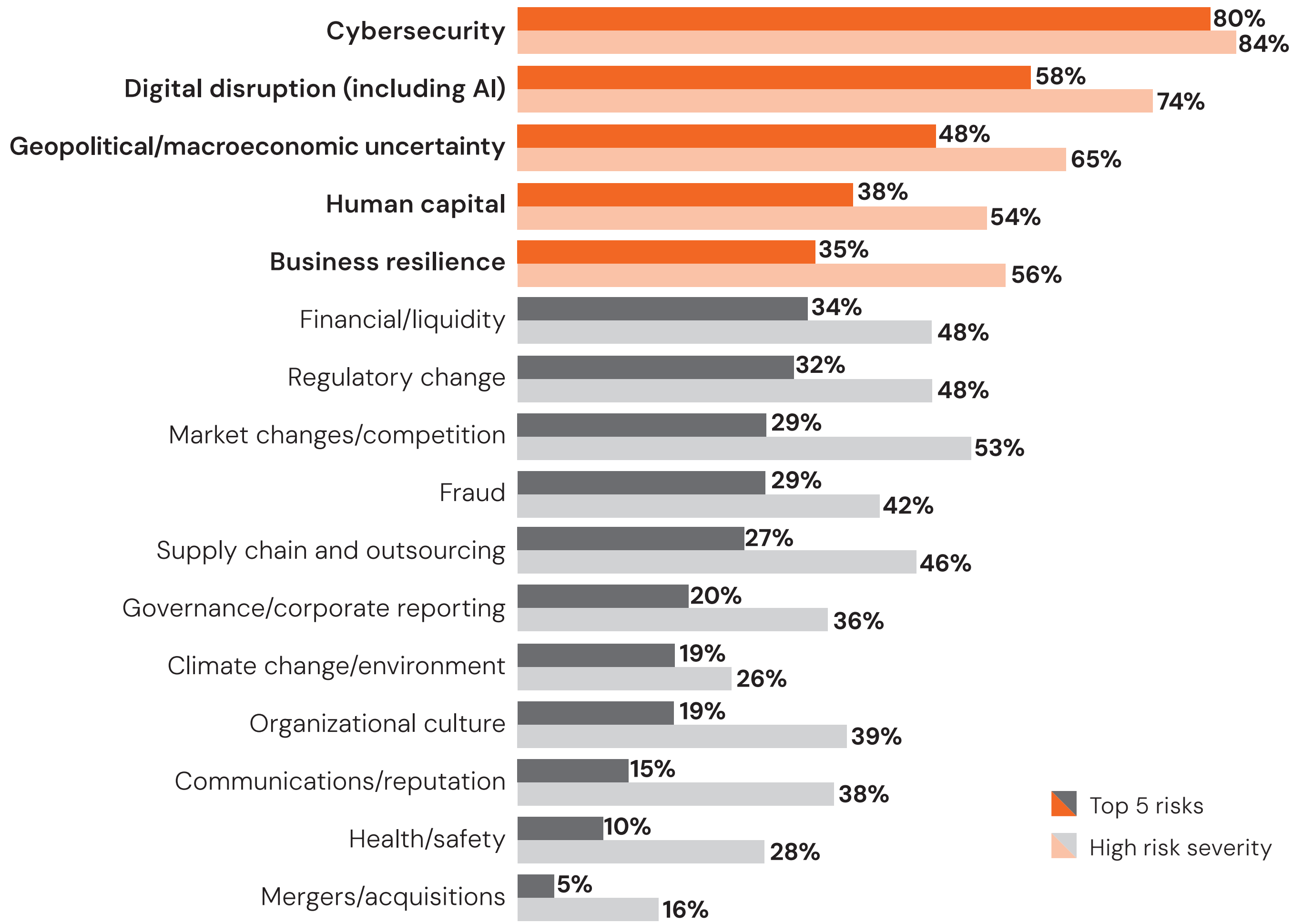
CAEs should consider structuring parts of the audit universe around risk pathways or scenarios. This helps internal audit identify common dependencies, cumulative exposures, weak handoffs, and controls that affect multiple risks.

"The defining feature of the 2027 risk landscape is not the rise of a single risk, but the speed at which technology, geopolitics, liquidity, fraud, and resilience now reinforce one another."

– Renato Trisciuzzi, Brazil

Exhibit 1.3. Global – Top 5 Risks vs. Risk Severity

Survey question 1: **What are the Top 5 risks your organization currently faces? (Choose 5.)**
Survey question 2: **On a scale of 1 to 7, please rate the current level of risk at your organization for each of the following risk areas.**



How to Interpret the Graph
Dark colors show who picked the risk as one of the 5 highest at their organization (Top 5 risk). **Light colors** show who rated the risk as a 5, 6, or 7 on a scale of 1 to 7 (high risk severity). Orange indicates the five highest ratings for both risk measures.

Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 3,285.

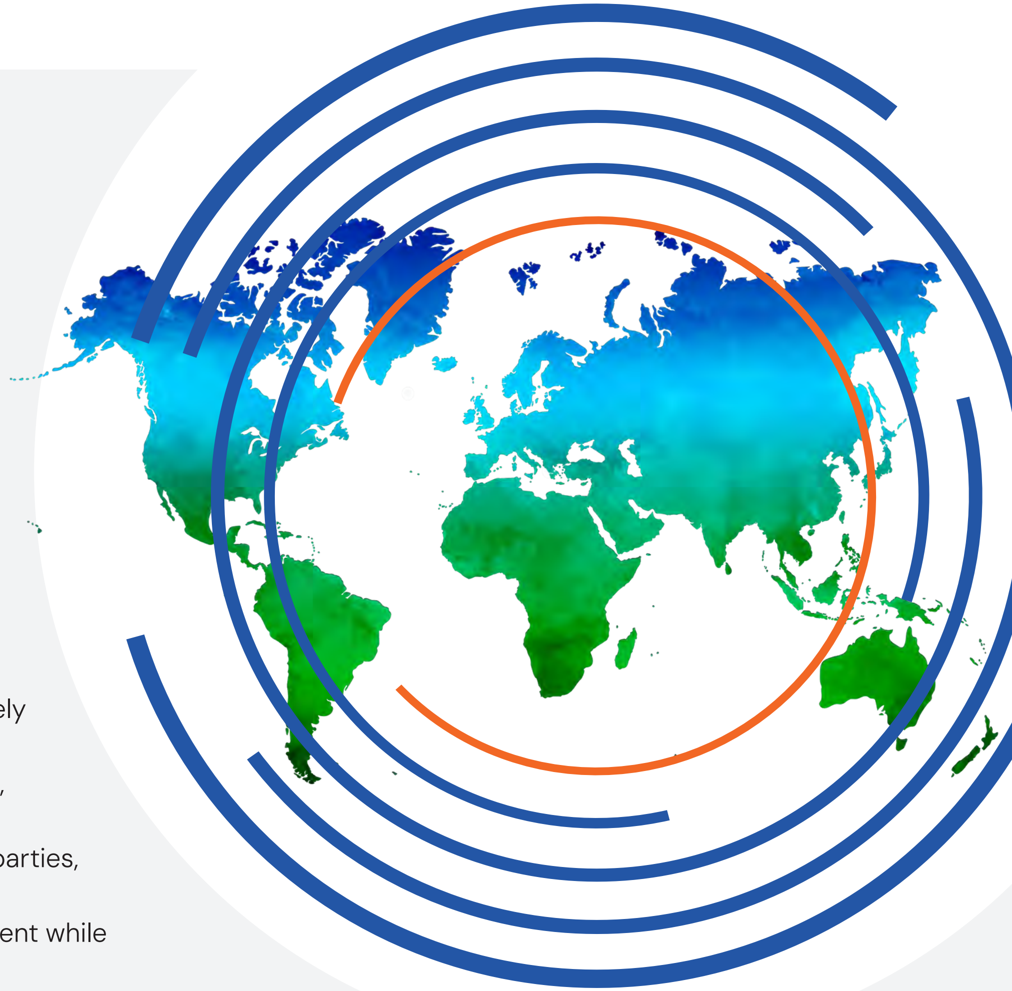
KEY POINTS

Survey insights

- Cybersecurity remains the dominant global risk at 80%.
- Digital disruption and geopolitical/macroeconomic uncertainty recorded the largest increases, both rising 10 percentage points.
- Business resilience, human capital, and market changes remain broadly significant even when they fall outside the five highest rankings.
- Regional differences show that common global risks materialize through different economic, regulatory, technological, and operational channels.
- When a risk is displaced from its Top 5 risk ranking, it may still retain high risk severity.

Internal audit strategies

- Assess interconnected risk scenarios rather than reviewing every risk exclusively within a separate silo.
- Translate external risks into organizational objectives, dependencies, decisions, processes, and response capabilities.
- Expand cybersecurity work to include AI, cloud, operational technology, third parties, resilience, recovery, communication, and fraud.
- Use global and regional comparisons to challenge management's risk assessment while maintaining organization-specific professional judgment.
- Present the board with both Top 5 rankings and risk severity ratings to reduce the risk of false comfort caused by risk displacement.



2. INTERNAL AUDIT PRIORITIES

Audit Effort Is Moving, But Legacy Priorities Remain

Internal audit functions are beginning to redirect effort toward the changing risk environment. However, established assurance obligations, regulatory requirements, legacy audit universes, familiar methodologies, and capability limitations continue to exert strong influence over audit plans. The critical question is not whether every risk receives equal coverage, but whether the allocation of scarce resources is deliberate, transparent, and responsive.

Alignment is strongest for cybersecurity

Cybersecurity shows the closest global alignment between risk and audit priority. It was selected as a Top 5 risk by 80% and as a Top 5 audit priority by 75% (Exhibit 2.1). Across regions, cybersecurity was rated as the most common Top 5 audit priority by a wide margin (Exhibit 2.3).

This is appropriate given the risk's scale, regulatory significance, stakeholder expectations, and potential systemic impact. Nevertheless, strong effort does not automatically mean coverage is sufficient or effective. The expanding attack surface and shortage of specialized skills can leave important elements under-assessed even where cybersecurity consumes substantial audit resources.

CAEs should therefore evaluate the nature and quality of coverage, not only the quantity of hours assigned.

Emerging-risk effort is increasing

Digital disruption recorded the largest increase in audit priority, rising 10 percentage points to 42% (Exhibit 2.2). It increased in every region and is now one of the five highest audit priorities in North America (53%), Latin America (47%), and the Middle East (43%) (Exhibit 2.3).

This movement is encouraging, but a 16-percentage-point gap remains between digital disruption risk and audit priority (Exhibit 2.1). Some functions lack the competencies or evaluation criteria needed for AI, automation, model risk, data governance, cloud platforms, digital products, or operational technology. Others may include digital work in existing engagements without identifying it as a separate priority.

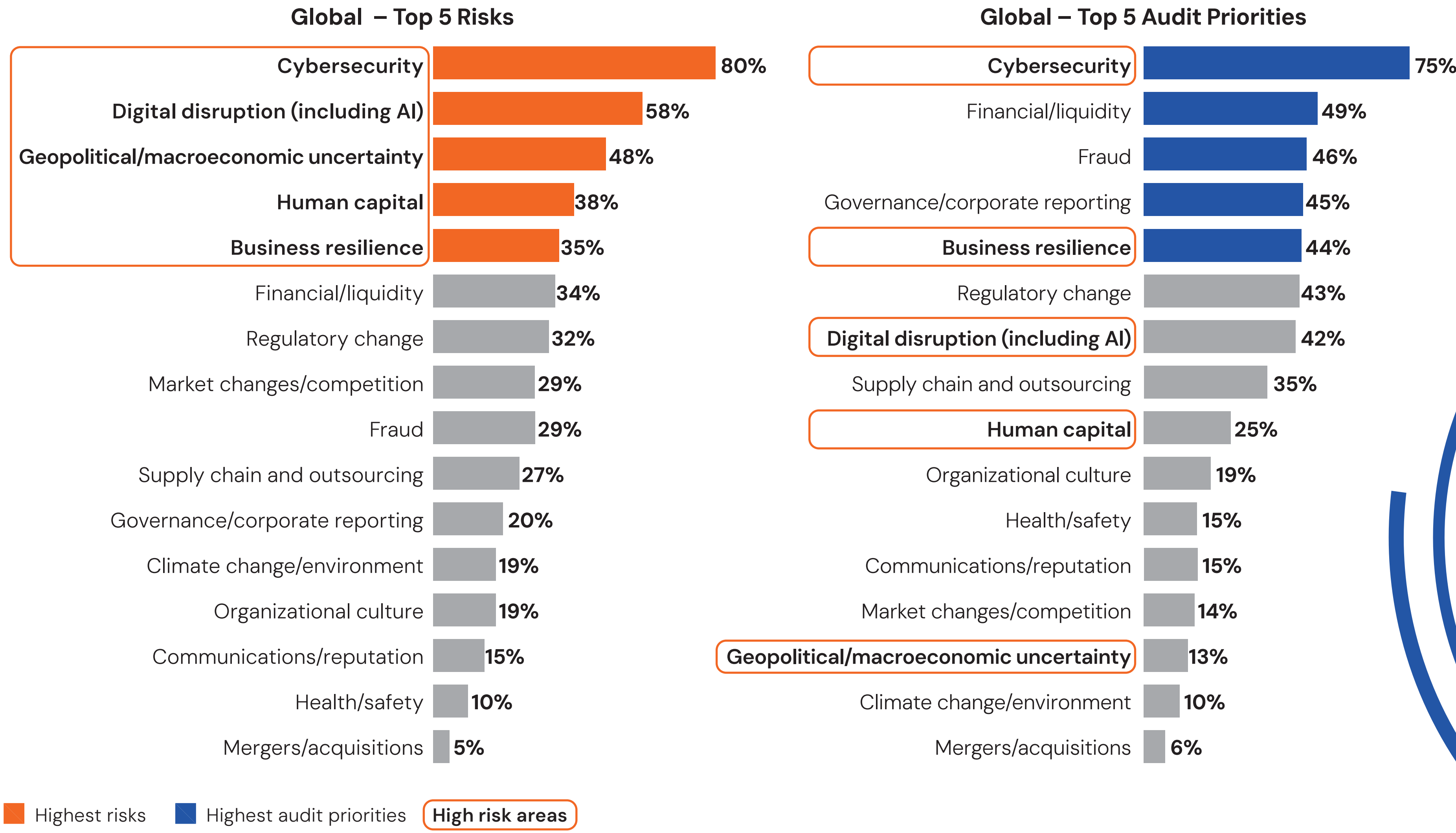
Digital disruption recorded the largest increase in audit priority, rising 10 percentage points to **42%**.

"Many audit plans still reflect what auditors know how to audit, rather than what most threatens the strategy."

– Ámbar Vargas, Panama

Exhibit 2.1. Global – Top 5 Risks vs. Top 5 Audit Priorities

Survey question 1: **What are the Top 5 risks your organization currently faces? (Choose 5.)**
Survey question 2: **What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)**



Note : Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 3,285.

The answer is not necessarily a single broad “AI audit.” CAEs can build coverage progressively through AI governance assessments, inventories, data governance reviews, third-party evaluations, model validation, cybersecurity procedures, pre-implementation advice, post-implementation assurance, and continuous monitoring.

The geopolitical gap requires translation

Geopolitical/macroeconomic uncertainty presents the largest global difference between risk and audit priority: 48% compared with 13% (Exhibit 2.1).

This does not mean that internal audit should attempt to audit geopolitical events themselves. Rather, the audit plan should address how management monitors and responds to their organizational consequences. Such work may be embedded in supply chain, treasury, liquidity, resilience, crisis management, strategic planning, regulatory compliance, third-party risk, energy security, workforce, or market entry engagements.

The Middle East has the highest regional audit priority for geopolitical uncertainty at 25%, reflecting the immediacy of regional conflict. By comparison, the priority is 15% in Africa, 14% in Latin America, 12% in Asia Pacific, 8% in Europe, and 6% in North America (Exhibit 2.3). These differences illustrate how proximity and immediacy influence audit planning.

Traditional areas retain substantial weight

As shown in Exhibit 2.1, internal audit priority exceeds the global risk ranking in several established areas:

- **Financial/liquidity:** 49% audit priority versus 34% risk
- **Fraud:** 46% versus 29%
- **Governance/corporate reporting:** 45% versus 20%
- **Business resilience:** 44% versus 35%
- **Regulatory change:** 43% versus 32%

These gaps should not automatically be interpreted as excess coverage. Financial, governance, regulatory, resilience, and fraud work may be required by law, regulation, board expectations, recurring assurance obligations, or past control failures.

However, the cumulative effect may reduce capacity for emerging risks. CAEs should periodically test whether historical coverage remains proportionate, whether work can be automated, whether reliance can be placed on other assurance providers, and whether engagement frequency can be adjusted.

Rebalancing audit priorities

The trend data in Exhibit 2.2 indicate that rebalancing has begun. Audit priority rose 6 percentage points for both cybersecurity and fraud, 5 for financial/liquidity, and 10 for digital disruption. At the same time, governance/corporate reporting declined 10 points and business resilience declined 9.

“Having more regular meetings with management and the board audit committee have reinforced internal audit’s role as a trusted strategic advisor.”

– Faiza Al Jabri, Oman

BACK NEXT CONTENTS

Exhibit 2.2. Global – Top 5 Audit Priorities Trend

Survey question: **What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)**

2023	2024	2025	2026	Change from 2025 to 2026	Change	Audit areas
68%	69%	69%	75%		+6	Cybersecurity
45%	45%	44%	49%		+5	Financial/liquidity
42%	41%	40%	46%		+6	Fraud
55%	56%	55%	45%		-10	Governance/corporate reporting
54%	55%	53%	44%		-9	Business resilience
46%	46%	46%	43%		-3	Regulatory change
22%	25%	32%	42%		+10	Digital disruption (including AI)
34%	31%	33%	35%		+2	Supply chain and outsourcing
30%	31%	29%	25%		-4	Human capital
24%	23%	23%	19%		-4	Organizational culture
17%	16%	15%	15%		0	Health/safety
20%	20%	18%	15%		-3	Communications/reputation
16%	16%	15%	14%		-1	Market changes/competition
9%	8%	11%	13%		+2	Geopolitical/macroeconomic uncertainty
11%	12%	10%	10%		0	Climate change/environment
6%	6%	5%	6%		+1	Mergers/acquisitions

Increased audit priority compared to prior year   Decreased audit priority compared to prior year

How to Interpret the Graph
Orange text indicates an increase of 4 percentage points or more compared to the prior year. The orange and blue bars show the difference in ratings from 2025 to 2026. The column labeled "change" shows the percentage point difference from 2025 to 2026.

Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 3,285.

INTERNAL AUDIT PRIORITIES

A strategy is more than an annual plan

The IIA's guidance distinguishes the internal audit strategy from the annual plan. The strategy provides the longer-term vision, objectives, capabilities, technology, stakeholder alignment, and initiatives needed for the function to fulfill its mandate. The plan translates current risk assessment into specific assurance and advisory work.

Both must remain connected to organizational strategy. A plan that is updated annually but supported by an outdated internal audit strategy may still lack the skills, technology, sourcing arrangements, or methodologies needed for emerging risks.

The IIA's guidance on risk-based planning also emphasizes responsiveness to changing risks. In volatile environments, CAEs should use quarterly refreshes, rolling plans, trigger-based reassessments, or reserved capacity for urgent work. The experience of Middle Eastern CAEs in creating "pop-up" advisory services during crisis illustrates how flexibility can preserve relevance without abandoning objectivity.

Capabilities should follow the risk profile

A risk-based plan cannot be executed without a risk-based capability model. CAEs should compare the audit universe with available skills in cybersecurity, data, AI, cloud, automation, operational technology, fraud, finance, supply chain, regulation, culture, and strategic risk.

Not every capability must be permanent. Options include training, recruitment, guest auditors, centers of excellence, co-sourcing, external specialists, and coordinated reliance on second-line functions. However, access to the capability should be established before a crisis makes it urgent.

"We played more of an advisory role in this phase to champion risk awareness and provide advice on evaluating the effectiveness of risk management around those threats."

– Roundtable participant, Egypt

Exhibit 2.3. Global – Top 5 Audit Priorities per Region

Survey question: **What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)**

Audit areas	Average of the regions	Africa	Asia Pacific	Europe	Latin America	Middle East	North America
Cybersecurity	**75% ↑**	**67% ↑**	**70% ↑**	**79% ↑**	**74% ↑**	**78% ↑**	**84%**
Financial/liquidity	**49% ↑**	**56% ↑**	**43% ↑**	**44%**	**52% ↑**	**52% ↑**	46%
Fraud	**46% ↑**	**57% ↑**	**48% ↑**	**42% ↑**	**56% ↑**	**38% ↑**	**35% ↑**
Governance/corporate reporting	**45%**	**43%**	**45%**	**45%**	38%	**53%**	**48%**
Business resilience	**44%**	**38%**	**51%**	**48%**	32%	**47%**	**51%**
Regulatory change	43%	33%	38%	**50%**	**53%**	32%	**54%**
Digital disruption (including AI)	**42% ↑**	**37% ↑**	**40% ↑**	**34% ↑**	**47% ↑**	**43% ↑**	**53% ↑**
Supply chain and outsourcing	35%	**35% ↑**	**42% ↑**	41%	27%	33%	34%
Human capital	25%	29%	27%	22%	26%	27%	**20% ↑**
Organizational culture	19%	22%	19%	17%	27%	18%	10%
Health/safety	15%	17%	15%	**21% ↑**	10%	13%	17%
Communications/reputation	15%	20%	13%	11%	16%	15%	14%
Market changes/competition	14%	13%	18%	10%	15%	15%	11%
Geopolitical/macroeconomic uncertainty	13%	**15% ↑**	**12% ↑**	8%	**14% ↑**	**25% ↑**	6%
Climate change/environment	10%	**18% ↑**	13%	11%	8%	8%	5%
Mergers/acquisitions	6%	2%	6%	6%	5%	5%	**11% ↑**

5 highest audit priorities

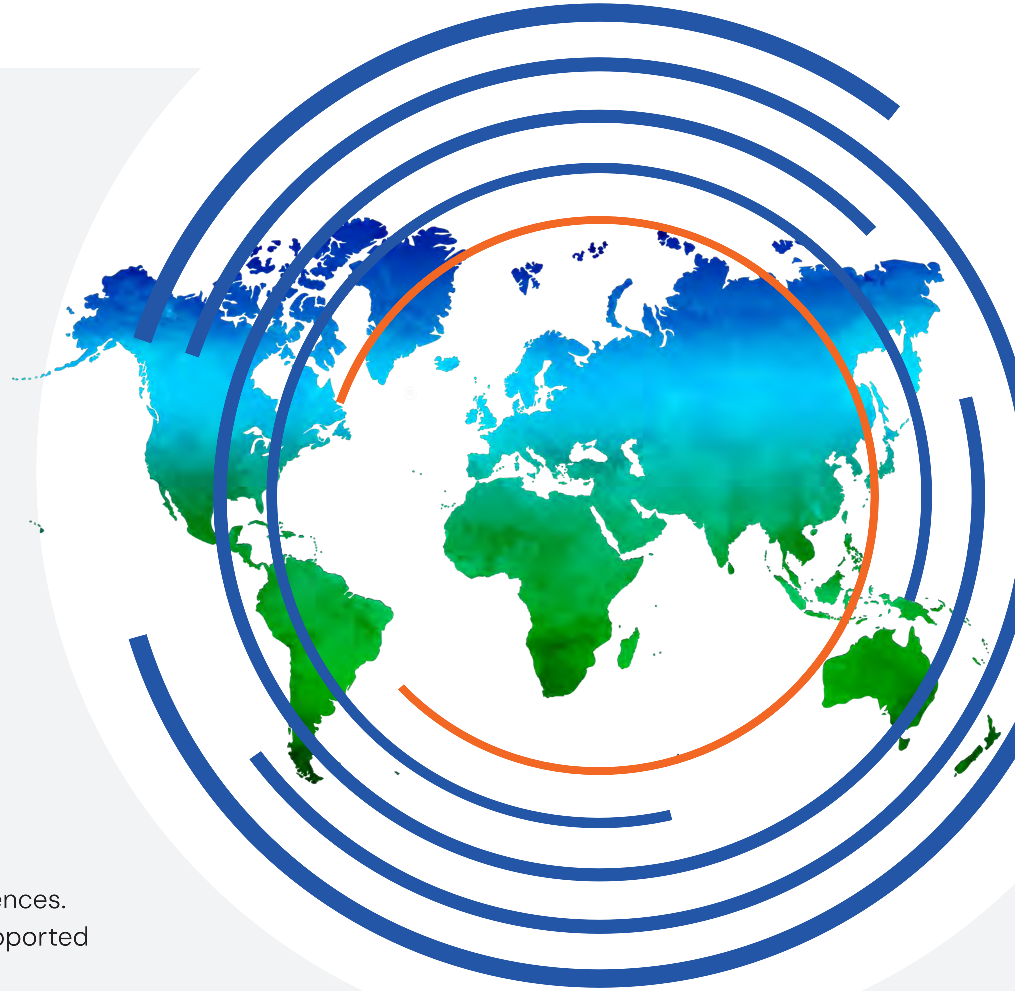
How to Interpret the Graph
The **red arrows** ↑ indicate an increase of 4 percentage points or more compared to the prior year.

Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 3,285.

KEY POINTS

Survey insights

- Cybersecurity is the strongest area of alignment between risk and audit priority.
- Digital disruption had the largest increase in audit effort, but coverage still trails risk.
- Geopolitical/macroeconomic uncertainty has the largest risk-to-priority gap.
- Traditional financial, governance, fraud, resilience, and regulatory work continues to shape audit plans worldwide.
- Audit priorities vary significantly by region, reflecting differences in exposure, regulation, maturity, and urgency.



Internal audit strategies

- Map Top 5 risks, high-risk severity, audit priority, assurance providers, and current coverage in one view.
- Rebalance audit priorities to align with risk trends.
- Establish formal refresh points and reserve capacity for emerging or rapidly changing risks.
- Translate geopolitical and market risks into auditable organizational consequences.
- Evaluate whether recurring audits can be automated, reduced, rotated, or supported through reliance on other providers.
- Maintain a capability plan that includes training, recruitment, co-sourcing, technology, and access to subject-matter expertise.
- Explain significant coverage gaps and resource constraints explicitly to the board.

3. RISK MATURITY AND COVERAGE

The Governance Blind Spot: High Risk, Low Maturity, Thin Coverage

Risk ranking shows exposure, but it does not show preparedness. Governance maturity indicates how effectively risk management is embedded in decision-making, while audit coverage indicates the extent of direct internal audit attention. Examining the three dimensions together reveals where risks may be accumulating faster than the organization's ability to manage or independently assess them.

Mature governance is concentrated in established areas

Financial/liquidity has the highest global risk governance maturity, with 62% rating it as managed or optimized. Governance/corporate reporting and regulatory change follow at 48%, cybersecurity at 45%, health/safety at 45%, communications/reputation at 44%, and fraud at 43% (Exhibit 3.1).

These areas often benefit from established ownership, regulatory expectations, tested frameworks, recurring reporting, documented controls, and experienced assurance providers.

By contrast, only 23% rated governance for digital disruption as managed or optimized. Climate change/environment also stands at 23%, while geopolitical/macroeconomic uncertainty reaches only 29% (Exhibit 3.1).

Emerging and externally driven risks are difficult to govern because ownership can be fragmented, reliable data may be limited, risk appetite may not be explicit, criteria may be immature, and the external environment can change faster than policies and controls.

Coverage is thinnest where uncertainty is greatest

Full internal audit coverage is highest for financial/liquidity at 47%, governance/corporate reporting at 40%, regulatory change and fraud at approximately 36%, and cybersecurity at 33% (Exhibit 3.1).

The lowest levels of full coverage are found in geopolitical/macroeconomic uncertainty at 10%, digital disruption at 11%, climate change/environment at 13%, and market changes/competition at 14% (Exhibit 3.1).

The combination of high risk, low maturity, and low coverage as evidenced in Exhibits 1.1 and 3.1 is particularly important:

- **Digital disruption:** 58% Top 5 risk, 23% mature governance, and 11% full coverage.
- **Geopolitical/macroeconomic uncertainty:** 48% Top 5 risk, 29% maturity, and 10% coverage.
- **Cybersecurity:** 80% Top 5 risk, 45% maturity, and 33% coverage.

Cybersecurity receives considerably more audit effort, but even there, the scale and pace of the risk exceed the percentages for mature governance and full coverage.

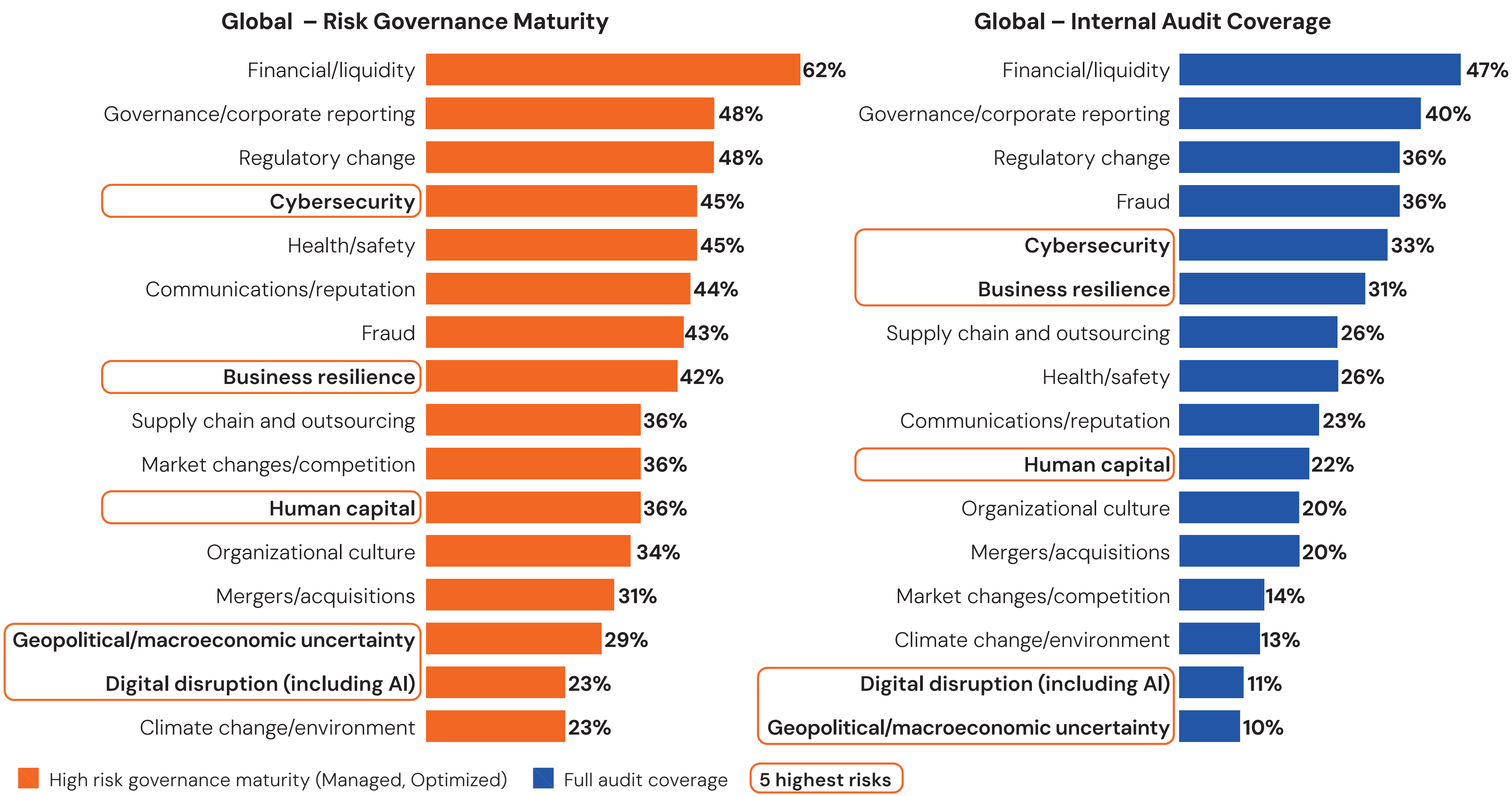
"Where risk governance functions effectively, it suggests that internal controls are already in place. That's why I question why internal auditors continue auditing areas where risk governance is already mature."

– Lilian Wangechi Mwangi, Africa

RISK MATURITY AND COVERAGE

Exhibit 3.1. Global – Risk Governance Maturity vs. Internal Audit Coverage

Survey question 1: **On a scale of 1 to 5, please rate the current level of risk governance maturity at your organization for each of the following risk areas.**
Survey question 2: **Please indicate the adequacy of internal audit's current coverage of these risk areas at your organization.**



How to Interpret the Graph
Response options for risk governance maturity were 1-Initial, 2-Infrastructure, 3-Integrated, 4-Managed, 5-Optimized. Response options for audit coverage adequacy were full coverage, partial coverage, and inadequate coverage.

Note : Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 3,285.

RISK MATURITY AND COVERAGE

Regional findings reinforce this concern. In Africa, digital disruption and geopolitical uncertainty each have only 10% full coverage. In North America, digital disruption has 9% full coverage and geopolitical uncertainty 15%. Europe similarly identifies geopolitical uncertainty and digital disruption as areas of high severity, low maturity, and weaker assurance coverage.

Low maturity requires a different response

Low maturity does not always support a conventional control-effectiveness audit. If ownership, governance, risk appetite, data, policies, and monitoring have not been established, there may be few mature controls to test.

In these circumstances, internal audit may provide greater value through:

- Governance design assessments.
- Readiness reviews.
- Risk and control workshops.
- Scenario and resilience testing.
- Maturity assessments.
- Pre-implementation advisory work.
- Reviews of accountability, escalation, and reporting.
- Benchmarking against appropriate frameworks.
- Follow-up assurance after management has implemented a response.

Internal audit should not design or own management's risk responses. However, timely advice can help management and the board understand gaps before they become control failures.

High maturity may create opportunities for reliance

Conversely, high maturity does not automatically mean internal audit should withdraw. The risk may remain critical, regulated, or highly consequential. Nevertheless, mature governance can create opportunities to refine engagement frequency, use continuous monitoring, rely on qualified second-line work, or focus on residual and systemic risk.

An analysis of risk maturity coverage can help the CAE distinguish among four situations:

1. **High risk, low maturity, low coverage:** Urgent need for governance attention, advisory support, capability building, and board visibility.
2. **High risk, high maturity, strong coverage:** Maintain appropriate assurance while seeking efficiency and reliance.
3. **Lower risk, high maturity, high coverage:** Assess whether resources can be reallocated.
4. **High risk, low direct coverage but strong assurance elsewhere:** Validate the reliability of other providers and communicate the total assurance position.

RISK MATURITY AND COVERAGE

Coordinate assurance across the Three Lines

The IIA's positions on ERM and the Three Lines reinforce distinct accountabilities. Management owns risk and operates controls. Second-line roles provide expertise, support, challenge, monitoring, and thematic review. Internal audit provides independent and objective assurance and advice without assuming management responsibility.

The CAE's organization-wide perspective and access to the board also position internal audit to facilitate assurance coordination. Assurance mapping can identify duplication, gaps, inconsistent risk conclusions, and areas where the board may be receiving either too much detail or too little assurance.

Coordination does not eliminate accountability. Reliance should be supported by an assessment of other providers' competence, objectivity, scope, methodology, and quality.

Make the gap visible to the board

CAEs should present more than a ranking of risks or a list of planned engagements. A concise board view can show, for each significant risk:

- Risk rating and trend.
- Governance maturity.
- Internal audit priority.
- Direct internal audit coverage.
- Coverage from other providers.
- Capability or resource constraints.
- Planned assurance or advisory response.
- Timing for reassessment.

This converts maturity and coverage data into a governance conversation. It also makes it explicit where management and the board are accepting limited assurance.

"A gap between risk, maturity, and coverage is not only an audit planning issue. It is a governance signal the board needs to see."

– Renato Trisciuzzi, Brazil

KEY POINTS

Survey insights

- Mature governance and strong coverage are concentrated in established financial, regulatory, governance, fraud, and cyber areas.
- Digital disruption and geopolitical/macroeconomic uncertainty combine high risk with low maturity and limited coverage.
- Climate and market risks also show comparatively low maturity or coverage.
- A high audit priority does not necessarily mean full or effective coverage.
- Direct internal audit coverage is only one component of the organization's total assurance position.

Internal audit strategies

- Create a map of risk maturity coverage assurance for discussion with the board.
- Use advisory and readiness work where governance is too immature for conventional control testing.
- Reassess engagement frequency and reliance where governance and assurance are mature.
- Coordinate with the second line and external assurance providers while validating the basis for reliance.
- Establish safeguards that preserve objectivity when internal audit advises on emerging governance arrangements.
- Report material assurance gaps, capability constraints, and accepted risks transparently.

CONCLUSION

The CAE as Architect of Adaptive Assurance

Risk in Focus 2026/2027 demonstrates that internal audit relevance depends on more than recognizing the highest risks. It depends on whether the function can interpret connected risks, adjust its priorities, mobilize the right capabilities, coordinate assurance, and provide the board with a clear view of where organizational exposure exceeds governance preparedness.

The global results tell a consistent story. Cybersecurity remains dominant. Digital disruption and geopolitical uncertainty are accelerating. Financial pressure, fraud, third parties, human capital, regulation, market change, and resilience interact with those risks and amplify their consequences.

Yet the most important finding is not the ranking itself. It is the mismatch that appears when risk, audit priority, governance maturity, and coverage are viewed together.

Internal audit has begun to respond. Effort has increased for cybersecurity, digital disruption, fraud, and financial/liquidity risk. But emerging and externally driven areas remain difficult to govern and audit. Traditional obligations continue to consume substantial capacity, while skills, methodologies, and data may lag behind the organization's changing risk profile.

CAEs can respond through four leadership priorities:

1. **Translate risk into organizational consequences.** External volatility becomes auditable through its effects on strategy, decisions, liquidity, supply chains, people, technology, continuity, and stakeholder trust.
2. **Build adaptive plans and capabilities.** The internal audit strategy should anticipate future skills and technology needs, while the audit plan should remain dynamic enough to respond to material changes.
3. **Integrate assurance without blurring accountability.** Internal audit should coordinate across the Three Lines, use reliance appropriately, and preserve independence and objectivity while providing timely advice.
4. **Make gaps visible.** Boards should understand not only which risks are highest, but also where governance is immature, assurance is thin, resources are constrained, or management has accepted exposure.

The strongest global internal audit functions will combine assurance with insight and foresight. They will remain sufficiently close to strategy to understand change, sufficiently objective to challenge it, and sufficiently agile to respond before emerging risks become organizational crises.

The question for 2027 is therefore not whether internal audit has identified the right risks. It is whether internal audit has positioned itself to help the organization act on them.

MORE GLOBAL RESOURCES

See Appendix D for valuable resources from The IIA related to risk and audit planning.

APPENDIX A. METHODOLOGY

Survey, Roundtables, and Interviews

The Internal Audit Foundation collected survey responses from March 24 to May 6, 2026, for all regions except Europe. Responses from Europe were collected by the European Institutes Research Group from March 2 to April 7, 2026.

Completed surveys were received from 3,285 internal auditors who confirmed that they were the highest-ranking internal auditor at their organizations. They represented 132 countries/locations. The survey was conducted online through contacts associated with IIA National Institutes and regional bodies. In addition, roundtables and interviews were conducted for each regional report.

The 16 risk areas used in the survey are shown below. Respondents were asked a variety of questions about risk levels, audit planning, and risk governance maturity.

Risk Name	Risk Description Used in the Survey
Business resilience	Business continuity, operational resilience, crisis management, and disaster response
Climate change/environment	Climate change, biodiversity, and environmental sustainability
Communications/reputation	Communications, reputation, and stakeholder relationships
Cybersecurity	Cybersecurity and data security
Digital disruption (including AI)	Digital disruption, new technology, and AI (artificial intelligence)
Financial/liquidity	Financial, liquidity, and insolvency risks
Fraud	Fraud, bribery, and the criminal exploitation of disruption
Geopolitical/macroeconomic uncertainty	Macroeconomic, social, and geopolitical uncertainty
Governance/corporate reporting	Organizational governance and corporate reporting
Health/safety	Health, safety, and security
Human capital	Human capital, diversity, and talent management and retention
Market changes/competition	Market changes/competition and customer behavior
Mergers/acquisitions	Mergers and acquisitions
Organizational culture	Organizational culture
Regulatory change	Change in laws and regulations
Supply chain and outsourcing	Supply chain, outsourcing, and 'nth' party risk

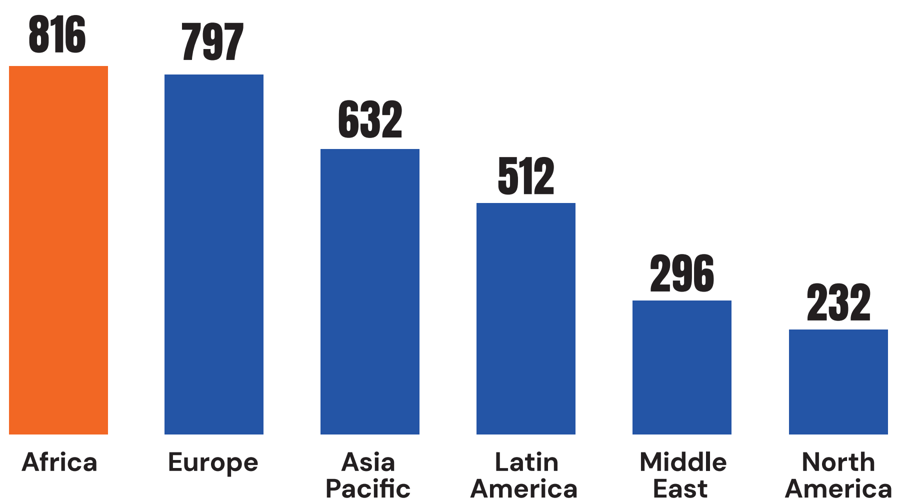
APPENDIX B. DEMOGRAPHICS

Exhibit B.1. Global – Response Rate per Region

GLOBAL TOTALS

3,285 respondents

132 countries/locations



Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 3,285.

APPENDIX C. RISK AND AUDIT PRIORITY TRENDS PER REGION

Exhibit C.1. Africa – Top 5 Risks Trend

Survey question: **What are the Top 5 risks your organization currently faces? (Choose 5.)**

2023	2024	2025	2026	Change from 2025 to 2026	Change	Risk areas
58%	64%	62%	73%		+11	Cybersecurity
33%	34%	44%	50%		+6	Digital disruption (including AI)
46%	42%	43%	50%		+7	Fraud
47%	42%	43%	49%		+6	Financial/liquidity
25%	23%	27%	35%		+8	Geopolitical/macroeconomic uncertainty
19%	25%	24%	31%		+7	Climate change/environment
39%	44%	35%	30%		–5	Human capital
32%	32%	34%	28%		–6	Regulatory change
52%	57%	49%	28%		–21	Business resilience
36%	31%	33%	27%		–6	Governance/corporate reporting
34%	34%	29%	26%		–3	Organizational culture
19%	16%	17%	21%		+4	Supply chain and outsourcing
21%	15%	19%	20%		+1	Market changes/competition
27%	26%	25%	18%		–7	Communications/reputation
10%	10%	11%	12%		+1	Health/safety
3%	4%	3%	2%		–1	Mergers/acquisitions

Increased risk compared to prior year   Decreased risk compared to prior year

How to Interpret the Graph

Orange text indicates an increase of 4 percentage points or more compared to the prior year. The orange and blue bars show the difference in ratings from 2025 to 2026. The column labeled "change" shows the percentage point difference from 2025 to 2026.

Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 816 for Africa.

Exhibit C.2. Africa – Top 5 Audit Priorities Trend

Survey question: **What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)**

2023	2024	2025	2026	Change from 2025 to 2026	Change	Audit areas
54%	**57%**	**60%**	**67%**		**+7**	**Cybersecurity**
57%	**49%**	**50%**	**57%**		**+7**	**Fraud**
53%	**55%**	**47%**	**56%**		**+9**	**Financial/liquidity**
52%	54%	51%	43%		-8	Governance/corporate reporting
56%	58%	54%	38%		-16	Business resilience
24%	**24%**	**30%**	**37%**		**+7**	**Digital disruption (including AI)**
32%	**29%**	**31%**	**35%**		**+4**	**Supply chain and outsourcing**
35%	39%	37%	33%		-4	Regulatory change
33%	36%	31%	29%		-2	Human capital
27%	25%	26%	22%		-4	Organizational culture
25%	25%	23%	20%		-3	Communications/reputation
11%	**9%**	**14%**	**18%**		**+4**	**Climate change/environment**
13%	**14%**	**13%**	**17%**		**+4**	**Health/safety**
12%	10%	12%	15%		+3	Geopolitical/macroeconomic uncertainty
15%	12%	13%	13%		0	Market changes/competition
2%	4%	3%	2%		-1	Mergers/acquisitions

Increased audit priority compared to prior year   Decreased audit priority compared to prior year

How to Interpret the Graph
Orange text indicates an increase of 4 percentage points or more compared to the prior year. The orange and blue bars show the difference in ratings from 2025 to 2026. The column labeled "change" shows the percentage point difference from 2025 to 2026.

Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 816 for Africa.

← BACK NEXT → CONTENTS

RISK AND AUDIT PRIORITY TRENDS PER REGION

Exhibit C.3. Asia Pacific – Top 5 Risks Trend

Survey question: **What are the Top 5 risks your organization currently faces? (Choose 5.)**

2023	2024	2025	2026	Change from 2025 to 2026	Change	Risk areas
66%	**64%**	**62%**	**72%**		**+10**	**Cybersecurity**
30%	**36%**	**39%**	**59%**		**+20**	**Digital disruption (including AI)**
28%	**30%**	**35%**	**48%**		**+13**	**Geopolitical/macroeconomic uncertainty**
61%	62%	58%	43%		-15	Business resilience
59%	57%	56%	41%		-15	Human capital
47%	49%	49%	37%		-12	Market changes/competition
27%	**24%**	**28%**	**33%**		**+5**	**Supply chain and outsourcing**
22%	**22%**	**20%**	**28%**		**+8**	**Fraud**
21%	**19%**	**19%**	**28%**		**+9**	**Financial/liquidity**
35%	32%	38%	24%		-14	Regulatory change
24%	22%	23%	21%		-2	Governance/corporate reporting
22%	26%	17%	20%		+3	Climate change/environment
23%	23%	21%	19%		-2	Organizational culture
18%	21%	19%	13%		-6	Communications/reputation
12%	11%	11%	8%		-3	Health/safety
4%	4%	6%	6%		0	Mergers/acquisitions

Increased risk compared to prior year   Decreased risk compared to prior year

How to Interpret the Graph
Orange text indicates an increase of 4 percentage points or more compared to the prior year. The orange and blue bars show the difference in ratings from 2025 to 2026. The column labeled "change" shows the percentage point difference from 2025 to 2026.

Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 632 for Asia Pacific.

RISK AND AUDIT PRIORITY TRENDS PER REGION

Exhibit C.4. Asia Pacific – Top 5 Audit Priority Trend

Survey question: **What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)**

2023	2024	2025	2026	Change from 2025 to 2026	Change	Audit areas
66%	**63%**	**63%**	**70%**		**+7**	**Cybersecurity**
59%	60%	57%	51%		-6	Business resilience
42%	**43%**	**42%**	**48%**		**+6**	**Fraud**
54%	55%	56%	45%		-11	Governance/corporate reporting
35%	**30%**	**30%**	**43%**		**+13**	**Financial/liquidity**
33%	**28%**	**32%**	**42%**		**+10**	**Supply chain and outsourcing**
19%	**23%**	**25%**	**40%**		**+15**	**Digital disruption (including AI)**
56%	52%	58%	38%		-20	Regulatory change
33%	33%	36%	27%		-9	Human capital
23%	25%	23%	19%		-4	Organizational culture
23%	25%	19%	18%		-1	Market changes/competition
18%	16%	17%	15%		-2	Health/safety
10%	16%	10%	13%		+3	Climate change/environment
21%	23%	18%	13%		-5	Communications/reputation
6%	**6%**	**7%**	**12%**		**+5**	**Geopolitical/macroeconomic uncertainty**
3%	2%	4%	6%		+2	Mergers/acquisitions

Increased audit priority compared to prior year   Decreased audit priority compared to prior year

How to Interpret the Graph

Orange text indicates an increase of 4 percentage points or more compared to the prior year. The orange and blue bars show the difference in ratings from 2025 to 2026. The column labeled "change" shows the percentage point difference from 2025 to 2026.

Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 632 for Asia Pacific.

Exhibit C.5. Europe – Top 5 Risks Trend

Survey question: **What are the Top 5 risks your organization currently faces? (Choose 5.)**

2023	2024	2025	2026	Change from 2025 to 2026	Change	Risk areas
84%	**83%**	**82%**	**86%**		**+4**	**Cybersecurity**
33%	**40%**	**47%**	**52%**		**+5**	**Digital disruption (including AI)**
43%	**39%**	**45%**	**51%**		**+6**	**Geopolitical/macroeconomic uncertainty**
43%	46%	45%	40%		-5	Regulatory change
57%	52%	48%	39%		-9	Human capital
35%	32%	39%	37%		-2	Business resilience
30%	32%	32%	32%		0	Market changes/competitions
26%	27%	27%	28%		+1	Financial/liquidity risks
30%	29%	29%	26%		-3	Supply chain and outsourcing
31%	33%	23%	21%		-2	Climate change/environment
20%	21%	19%	17%		-2	Organizational culture
12%	**14%**	**12%**	**17%**		**+5**	**Communications/reputation**
13%	14%	16%	16%		0	Fraud
22%	20%	20%	13%		-7	Governance/corporate reporting
13%	12%	12%	12%		0	Health/safety
8%	8%	5%	5%		0	Mergers/acquisitions

Increased risk compared to prior year   Decreased risk compared to prior year

How to Interpret the Graph
Orange text indicates an increase of 4 percentage points or more compared to the prior year. The orange and blue bars show the difference in ratings from 2025 to 2026. The column labeled "change" shows the percentage point difference from 2025 to 2026.

Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 797 for Europe.

Exhibit C.6. Europe – Top 5 Audit Priority Trend

Survey question: **What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)**

2023	2024	2025	2026	Change from 2025 to 2026	Change	Audit areas
79%	**74%**	**72%**	**79%**		**+7**	**Cybersecurity**
50%	51%	49%	50%		+1	Regulatory change
50%	47%	50%	48%		-2	Business resilience
61%	64%	58%	45%		-13	Governance/corporate reporting
45%	40%	43%	44%		+1	Financial/liquidity
36%	**36%**	**37%**	**42%**		**+5**	**Fraud**
36%	36%	39%	41%		+2	Supply chain and outsourcing
21%	**23%**	**29%**	**34%**		**+5**	**Digital disruption (including AI)**
26%	28%	27%	22%		-5	Human capital
19%	**18%**	**17%**	**21%**		**+4**	**Health/safety**
21%	24%	21%	17%		-4	Organizational culture
19%	20%	16%	11%		-5	Climate change/environment
11%	14%	14%	11%		-3	Communications/reputation
10%	13%	13%	10%		-3	Market changes/competition
8%	6%	8%	8%		0	Geopolitical/macroeconomic uncertainty
9%	7%	5%	6%		+1	Mergers/acquisitions

Increased audit priority compared to prior year   Decreased audit priority compared to prior year

How to Interpret the Graph
Orange text indicates an increase of 4 percentage points or more compared to the prior year. The orange and blue bars show the difference in ratings from 2025 to 2026. The column labeled "change" shows the percentage point difference from 2025 to 2026.

Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 797 for Europe.

Exhibit C.7. Latin America – Top 5 Risks Trend

Survey question: **What are the Top 5 risks your organization currently faces? (Choose 5.)**

2023	2024	2025	2026	Change from 2025 to 2026	Change	Risk areas
75%	74%	76%	80%		+4	Cybersecurity
38%	37%	54%	61%		+7	Digital disruption (including AI)
42%	37%	45%	52%		+7	Geopolitical/macroeconomic uncertainty
30%	32%	32%	38%		+6	Fraud
44%	46%	40%	37%		−3	Human capital
48%	45%	49%	36%		−13	Regulatory change
33%	33%	32%	36%		+4	Financial/liquidity
26%	26%	24%	27%		+3	Market changes/competition
26%	28%	28%	26%		−2	Organizational culture
47%	49%	35%	25%		−10	Business resilience
22%	29%	25%	23%		−2	Climate change/environment
16%	17%	15%	17%		+2	Supply chain and outsourcing
18%	18%	16%	15%		−1	Governance/corporate reporting
22%	17%	19%	15%		−4	Communications/reputation
8%	9%	6%	7%		+1	Health/safety
3%	4%	5%	4%		−1	Mergers/acquisitions

Increased risk compared to prior year   Decreased risk compared to prior year

How to Interpret the Graph
Orange text indicates an increase of 4 percentage points or more compared to the prior year. The orange and blue bars show the difference in ratings from 2025 to 2026. The column labeled "change" shows the percentage point difference from 2025 to 2026.

Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 512 for Latin America.

Exhibit C.8. Latin America – Top 5 Audit Priority Trend

Survey question: **What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)**

2023	2024	2025	2026	Change from 2025 to 2026	Change	Audit areas
66%	**67%**	**69%**	**74%**		**+5**	**Cybersecurity**
47%	**52%**	**51%**	**56%**		**+5**	**Fraud**
50%	49%	51%	53%		+2	Financial/liquidity
50%	47%	53%	53%		0	Regulatory change
24%	**19%**	**29%**	**47%**		**+18**	**Digital disruption (including AI)**
46%	46%	48%	38%		-10	Governance/corporate reporting
53%	49%	40%	32%		-8	Business resilience
29%	30%	29%	27%		-2	Organizational culture
28%	29%	24%	27%		+3	Supply chain and outsourcing
28%	29%	27%	26%		-1	Human capital
23%	22%	20%	16%		-4	Communications/reputation
17%	17%	16%	15%		-1	Market changes/competition
13%	12%	16%	14%		-2	Geopolitical and macroeconomic uncertainty
12%	14%	12%	10%		-2	Health/safety
8%	11%	9%	8%		-1	Climate change/environment
5%	7%	6%	5%		-1	Mergers/acquisitions

Increased audit priority compared to prior year   Decreased audit priority compared to prior year

How to Interpret the Graph
Orange text indicates an increase of 4 percentage points or more compared to the prior year. The orange and blue bars show the difference in ratings from 2025 to 2026. The column labeled "change" shows the percentage point difference from 2025 to 2026.

Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 512 for Latin America.

Exhibit C.9. Middle East – Top 5 Risks Trend

Survey question: **What are the Top 5 risks your organization currently faces? (Choose 5.)**

2023	2024	2025	2026	Change from 2025 to 2026	Change	Risk areas
70%	66%	72%	81%		+9	Cybersecurity
16%	27%	29%	60%		+31	Geopolitical/macroeconomic uncertainty
32%	38%	50%	58%		+8	Digital disruption (including AI)x
53%	63%	58%	47%		-11	Business resilience
38%	38%	38%	42%		+4	Financial/liquidity
28%	26%	23%	35%		+12	Supply chain and outsourcing
46%	43%	38%	34%		-4	Human capital
45%	41%	38%	27%		-11	Governance/corporate reporting
27%	27%	19%	22%		+3	Fraud
33%	27%	28%	20%		-8	Regulatory change
27%	29%	29%	20%		-9	Market changes/competition
10%	12%	13%	15%		+2	Climate change/environment
28%	21%	19%	13%		-6	Communications/reputation
30%	21%	26%	13%		-13	Organizational culture
9%	12%	11%	10%		-1	Health/safety
10%	8%	6%	3%		-3	Mergers/acquisitions

Increased risk compared to prior year   Decreased risk compared to prior year

How to Interpret the Graph

Orange text indicates an increase of 4 percentage points or more compared to the prior year. The orange and blue bars show the difference in ratings from 2025 to 2026. The column labeled "change" shows the percentage point difference from 2025 to 2026.

Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 296 for Middle East.

← BACK NEXT → CONTENTS

Exhibit C.10. Middle East – Top 5 Audit Priority Trend

Survey question: **What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)**

2023	2024	2025	2026	Change from 2025 to 2026	Change	Audit areas
61%	**65%**	**69%**	**78%**		**+9**	**Cybersecurity**
64%	58%	64%	53%		-11	Governance/corporate reporting
43%	**50%**	**47%**	**52%**		**+5**	**Financial/liquidity**
53%	61%	59%	47%		-12	Business resilience
20%	**30%**	**36%**	**43%**		**+7**	**Digital disruption (including AI)**
43%	**37%**	**30%**	**38%**		**+8**	**Fraud**
40%	31%	35%	33%		-2	Supply chain and outsourcing
35%	32%	30%	32%		+2	Regulatory change
34%	37%	35%	27%		-8	Human capital
8%	**9%**	**13%**	**25%**		**+12**	**Geopolitical/macroeconomic uncertainty**
27%	24%	19%	18%		-1	Organizational culture
23%	19%	19%	15%		-4	Communications/reputation
16%	19%	14%	15%		+1	Market changes/competition
16%	16%	14%	13%		-1	Health/safety
7%	6%	8%	8%		0	Climate change/environment
9%	7%	4%	5%		+1	Mergers/acquisitions

Increased audit priority compared to prior year   Decreased audit priority compared to prior year

How to Interpret the Graph

Orange text indicates an increase of 4 percentage points or more compared to the prior year. The orange and blue bars show the difference in ratings from 2025 to 2026. The column labeled “change” shows the percentage point difference from 2025 to 2026.

Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 296 for Middle East.

RISK AND AUDIT PRIORITY TRENDS PER REGION

Exhibit C.11. North America – Top 5 Risks Trend

Survey question: **What are the Top 5 risks your organization currently faces? (Choose 5.)**

2023	2024	2025	2026	Change from 2025 to 2026	Change	Risk areas
85%	87%	86%	85%		–1	Cybersecurity
36%	**48%**	**53%**	**69%**		**+16**	**Digital disruption (including AI)**
65%	54%	42%	45%		+3	Human capital
28%	26%	45%	43%		–2	Geopolitical/macroeconomic uncertainty
43%	47%	51%	42%		–9	Regulatory change
41%	**41%**	**34%**	**41%**		**+7**	**Market changes/competition**
36%	29%	30%	33%		+3	Supply chain and outsourcing
36%	41%	46%	29%		–17	Business resilience
28%	28%	27%	24%		–3	Financial/liquidity
9%	**9%**	**11%**	**18%**		**+7**	**Fraud**
21%	20%	18%	16%		–2	Communications/reputation
21%	20%	20%	16%		–4	Organizational culture
16%	16%	15%	14%		–1	Governance/corporate reporting
17%	13%	8%	11%		+3	Health/safety
12%	13%	7%	7%		0	Climate change/environment
8%	8%	7%	7%		0	Mergers/acquisitions

Increased risk compared to prior year   Decreased risk compared to prior year

How to Interpret the Graph
Orange text indicates an increase of 4 percentage points or more compared to the prior year. The orange and blue bars show the difference in ratings from 2025 to 2026. The column labeled "change" shows the percentage point difference from 2025 to 2026.

Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 232 for North America.

Exhibit C.12. North America – Top 5 Audit Priority Trend

Survey question: **What are the Top 5 audit areas on which internal audit spends the most time and effort? (Choose 5.)**

2023	2024	2025	2026	Change from 2025 to 2026	Change	Audit areas
84%	87%	84%	84%		0	Cybersecurity
53%	54%	51%	54%		+3	Regulatory change
25%	**33%**	**44%**	**53%**		**+9**	**Digital disruption (including AI)**
53%	54%	60%	51%		-9	Business resilience
55%	58%	52%	48%		-4	Governance/corporate reporting
46%	46%	44%	46%		+2	Financial/liquidity
26%	**29%**	**30%**	**35%**		**+5**	**Fraud**
38%	34%	37%	34%		-3	Supply chain and outsourcing
26%	**27%**	**15%**	**20%**		**+5**	**Human capital**
21%	16%	15%	17%		+2	Health/safety
20%	17%	14%	14%		0	Communications/reputation
10%	**10%**	**7%**	**11%**		**+4**	**Mergers/acquisitions**
14%	10%	14%	11%		-3	Market changes/competition
17%	15%	18%	10%		-8	Organizational culture
4%	3%	11%	6%		-5	Geopolitical/macroeconomic uncertainty
9%	9%	3%	5%		+2	Climate change/environment

Increased audit priority compared to prior year   Decreased audit priority compared to prior year

How to Interpret the Graph
Orange text indicates an increase of 4 percentage points or more compared to the prior year. The orange and blue bars show the difference in ratings from 2025 to 2026. The column labeled "change" shows the percentage point difference from 2025 to 2026.

Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 232 for North America.

APPENDIX D. IIA RESOURCES

The IIA offers a variety of resources to support internal auditors with risk assessment and audit planning through the Standards and Guidance department. Most of these resources are available free to IIA members worldwide, and some are also available to the public at large. To see the most recent releases, visit the Global Guidance resource page and the Statements of Position release page.

Risk Environment

- Assessing the Risk Management Process, 2nd Edition (The IIA, Global Practice Guide, 2024)
- Role of the Internal Audit Function in Enterprise Risk Management (The IIA, Statement of Position, 2026)

Audit Priorities

- AI Framework Support Tools (The IIA, Audit Tools, 2026)
- Artificial Intelligence Auditing Framework (The IIA, 2024)
- Auditing Cybersecurity Operations: Prevention and Detection, 2nd Edition (The IIA, Global Practice Guide, 2025)
- Auditing Privacy and Data Protection Risks, 3rd Edition (The IIA, Global Practice Guide, 2026)
- Internal Auditing and Fraud, 3rd Edition (The IIA, Global Practice Guide, 2024)
- Organizational Resilience Topical Requirement (The IIA, Topical Requirement, 2026)

Risk Governance Maturity and Internal Audit Coverage

- Developing a Risk-Based Internal Audit Plan, 2nd Edition (The IIA, Global Practice Guide, 2025)
- Developing an Internal Audit Strategy (The IIA, Global Practice Guide, 2025)
- Three Lines Model (The IIA, Statement of Position, 2026)

Global Internal Audit Standards

- Complete Global Internal Audit Standards
- Condensed Global Internal Audit Standards

INTERNAL AUDIT FOUNDATION

The Internal Audit Foundation is the preeminent global resource, in strategic partnership with The IIA, dedicated to elevating and empowering the internal audit profession by developing cutting-edge research and programs. For 50 years, the Foundation has helped current and future internal auditors stay relevant by building and enhancing their skills and knowledge, ensuring organizations are equipped to create, protect, and sustain long-term value. Visit theiia.org/Foundation.

50 Internal Audit FOUNDATION 1976-2026

Research Team

Research lead
Deborah Poulalion,
Senior Manager, Research and Insights, The IIA

Project manager
Candace Sacher

Writer
Renato Trisciuzzi, CIA, QIAL, CCSA, CRMA, MSc, PhD

Graphic designers
Sergio Analco and
Cathy Watanabe

INTERNAL AUDIT FOUNDATION PARTNERS

DIAMOND PARTNERS

bakertilly

Deloitte.

Grant Thornton

KPMG

Optro

The Institute of Internal Auditors

The Institute of Internal Auditors *Chicago*

Wolters Kluwer

GOLD PARTNERS

- Carr, Riggs & Ingram
- Fundación Latinoamericana de Auditores Internos
- IIA–Houston Chapter
- IIA–Japan
- IIA–New York Chapter
- IIA–San Francisco Chapter

PRESIDENT'S CIRCLE

(Individual Donors)

- Larry Harrington, CIA, QIAL, CRMA
- Glenn Ho, CIA, CRMA
- Keith Kahl, CIA, CRMA
- Doug Mims, CIA, CRMA
- Jessica Rodgers, CIA
- Stacey Schabel, CIA
- Michael A. Smith, CIA
- Warren Stippich, CIA, CRMA

THE IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 265,000 global members and has awarded more than 200,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

Disclaimer and Copyright

September 2026

The Institute of
Internal Auditors

Global Headquarters | The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401 | Lake Mary, FL 32746, USA
Phone: +1-407-937-1111 | Fax: +1-407-937-1101
Web: theiia.org