NORTH AMERICA 2026/2027

Hot Topics for Internal Auditors

RISK in FOCUS

Optro

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.

GLOBAL RESEARCH PARTICIPATION

132 countries/ territories

3,285 survey responses

17 roundtables with **149** participants

12 in-depth interviews

Internal Audit FOUNDATION 1976-2026

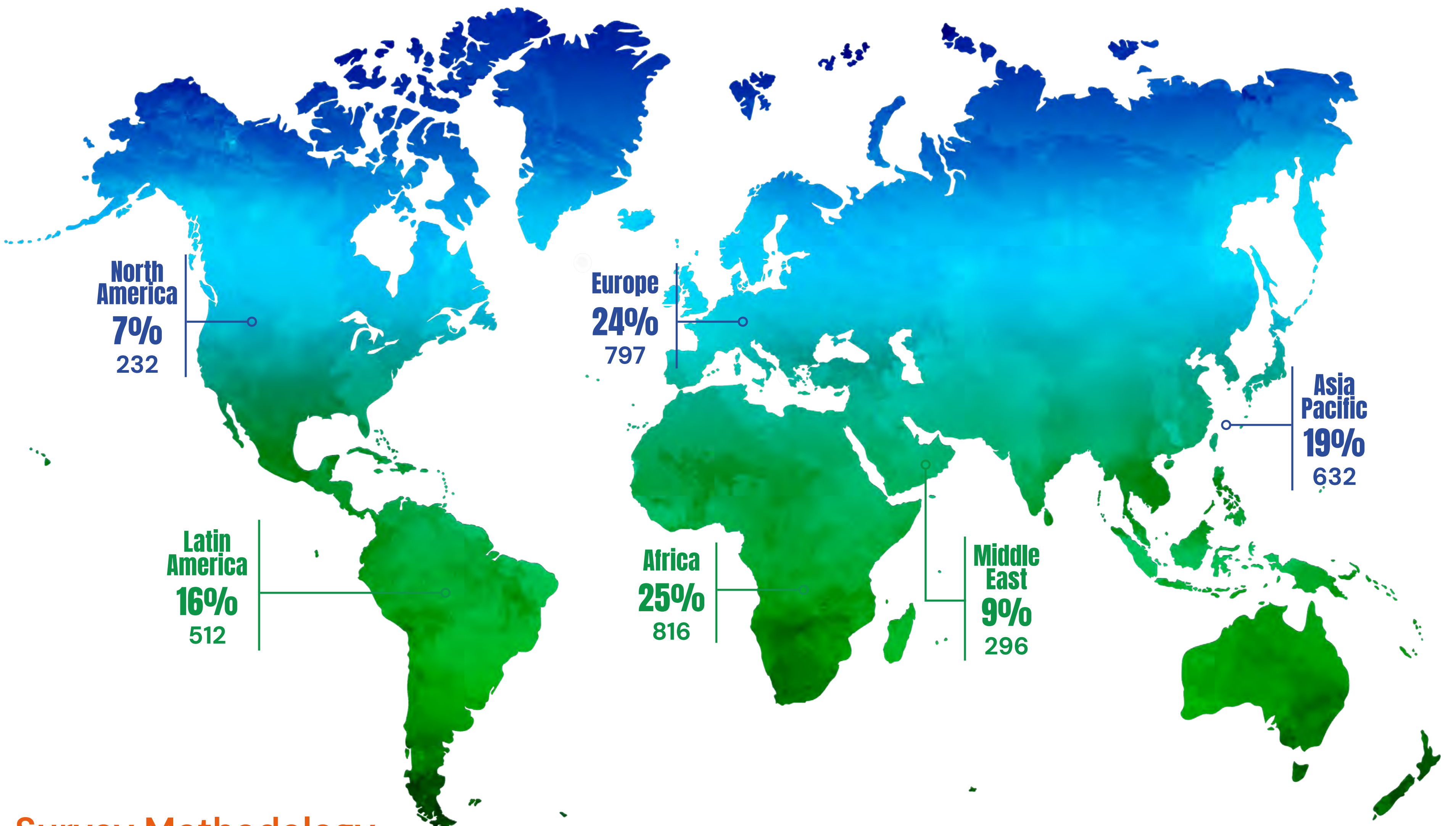
Visit the Risk in Focus Knowledge Center for free reports and board briefings (theiia.org/RiskInFocus).

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

Risk Volatility Drives Changes in Audit Activities

While risk volatility is virtually assured in the current geopolitical, economic, and digital landscapes, audit leaders are monitoring these rapid changes and tailoring their activities to address the areas of greatest impact for their organizations.

Based on the 2026/2027 North American survey, the three highest risk areas facing survey respondents' organizations were:

- **Cybersecurity.** Cybersecurity remained entrenched as the most cited risk in North America with 85% of respondents ranking it as a Top 5 risk, with little change compared to the prior year (Exhibit 1.1).
- **Digital disruption.** Digital disruption (including AI) boosted its risk ranking 16 percentage points over last year, to reach an all-time high (Exhibit 1.2). Digital disruption is increasingly viewed as pervasive in its influence over other risk categories.
- **Human capital.** CAEs cite AI as a key factor for this risk area, as organizations face challenges with incorporating AI into their human capital strategy.
- **Geopolitical uncertainty.** Political change remains a top risk in North America, cited by 43% of respondents, after the dramatic increase in the prior year.
- **Regulatory change.** Even though risk ratings for regulatory change fell substantially, this traditional audit area is still considered high risk for North America.

New strategies

Internal audit functions are adapting new strategies to respond to emerging risks, but much effort continues to be allocated to traditional audit areas.

- **AI focus increasing.** Digital disruption is taking a larger portion of internal audit's focus in North America, more than doubling in the past four years (from 25% to 53%) (Exhibit 2.2). Audit functions are incorporating AI into internal audit activities in order to increase efficiency and enable continuous monitoring.
- **Political impact monitored through reviews of related risks.** Audit leaders are monitoring and planning for geopolitical impacts on supply chain, regulatory change, business resilience, finances, and market changes.
- **High emphasis on compliance.** A large part of internal audit's priorities remains on compliance work. Governance/corporate reporting and regulatory change remained among the Top 5 areas where internal audit spends most of its time and effort.

Finally, internal audit coverage and risk governance maturity are important to consider together, especially for emerging risks. Of greatest concern are high-risk areas that fared poorly for both governance maturity and audit coverage, specifically digital disruption and geopolitical uncertainty.

NORTH AMERICA RESEARCH PARTICIPATION

232 survey responses

9 countries/locations*

2 roundtables

3 in-depth interviews

PROJECT SPONSOR

Optro

* Responses were primarily from the U.S. and Canada. English-speaking countries from the Caribbean are also included.

1. RISK ENVIRONMENT

Technology and Political Change Shape the Risk Landscape

Cybersecurity and digital disruption dominated the Top 5 risk rankings in North America, with digital disruption rising 16 percentage points over the prior year (Exhibit 1.2).

Human capital, geopolitical uncertainty, and regulatory change rounded out the Top 5 highest ranked risks, with market changes/competition coming in a close sixth (Exhibit 1.1).

Notably, respondents listing fraud as a Top 5 risk rose from 11% to 18% (Exhibit 1.2).

Recognizing risk displacement

Exhibit 1.1 provides a useful comparison between Top 5 risk rankings and risk severity rated on a scale of 1 to 7. It is particularly helpful in recognizing the impact of choice displacement, where some risks drop in the Top 5 risk ranking as more urgent, emerging risks take their place. For example, while 29% of respondents ranked business resilience as a Top 5 risk, nearly half (47%) rated the risk severity as high, very high, or extremely high. Similarly, 33% of survey respondents ranked supply chain as a Top 5 risk, but nearly half (47%) rated the risk severity as high, very high, or extremely high.

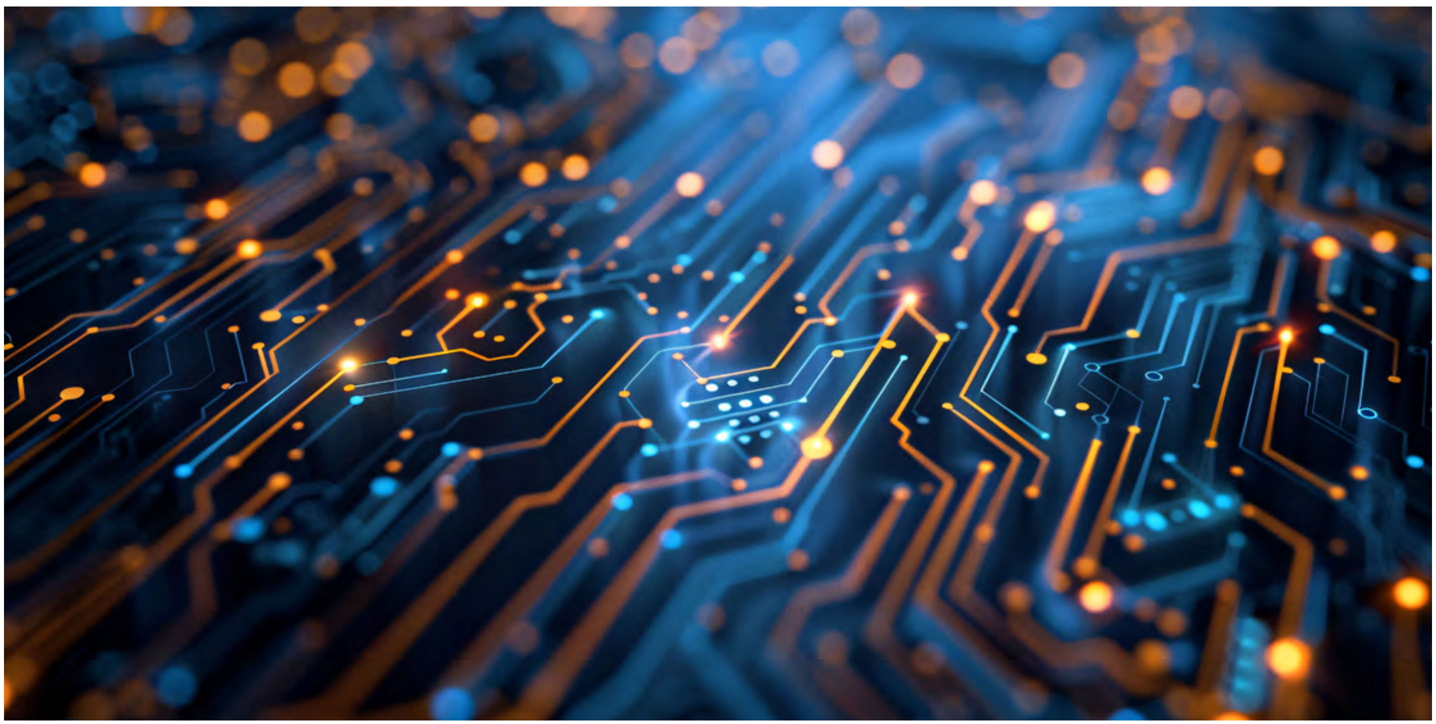
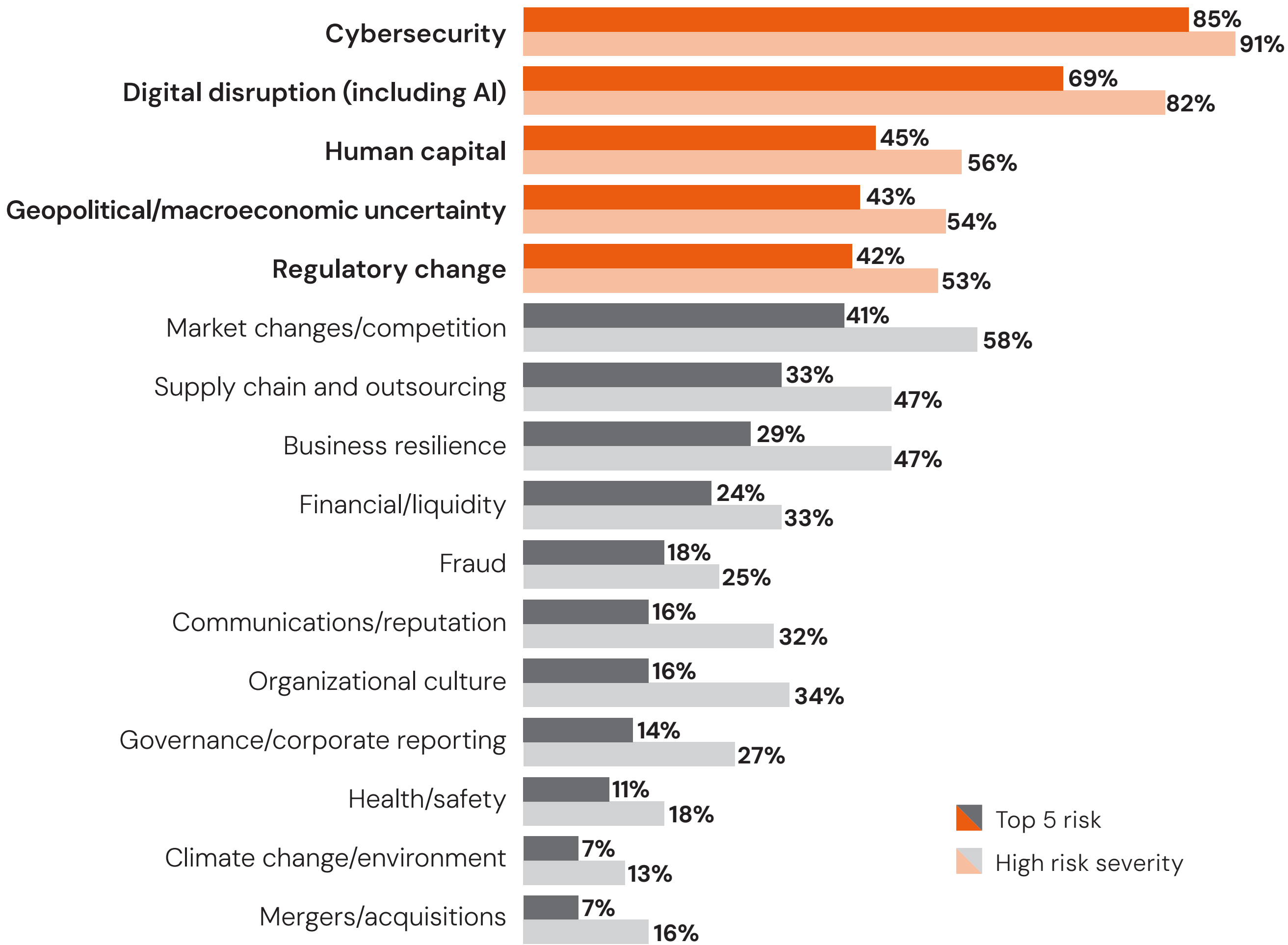


Exhibit 1.1. North America – Top 5 Risks vs. High Risk Severity

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* = 232 for North America.

Digital disruption's impact on other risks

Practitioners and subject-matter experts point to AI adoption rates outpacing supporting governance as a major driver of concern as well as persistent apprehension about internal audit's ability to provide effective risk assurance and advisory services in this risk area. Over a four-year period, risk ratings for digital disruption rose from 36% in 2023 to 69% in 2026.

Audit leaders are increasingly attuned to the effects of digital disruption on other risk areas, including cybersecurity, supply chain, third-party risk management, fraud, human capital, and business resilience.

AI is fundamentally changing cybersecurity itself. AI is increasingly enabling more sophisticated phishing, impersonation, and automated attacks, and changing how organizations detect and respond to threats. AI is a key driver of cybersecurity risks.

But AI's impact doesn't stop at cybersecurity. For example, a roundtable participant commented that software supply chain risk is particularly high for financial institutions. Brian Tremblay, an audit leader at a major defense contractor, warned that supply chain risk has evolved over time to include, and in some cases be dominated by, software, which many companies may not appreciate or even realize.

Similarly, third-party vendors face digital disruption risks, and that risk is passed along to their clients. Indeed, the concentration of risks with third and fourth parties, especially when it comes to data warehousing, should be of concern, another financial services audit leader noted.

Roundtable participants said the growth in digital disruption risk is impacting human capital risk, as well. "The AI emergence is making the human capital risk even greater," said the head of internal audit at a publicly traded energy company. "Concerns by employees about job loss, concerns about how to train and upskill, I think it's injected a lot of complexity into that space."

From the internal audit staffing perspective, the head of internal audit at a privately held public amenity in Canada noted that attracting data engineers and AI specialists has become nearly impossible for mid-size private companies.

Fraud

Fraud rankings jumped 7% year over year in North America, reflecting both increased incidents of AI-supported fraud and pressure on public sector auditors in the U.S. to crack down on fraud in federally funded social support programs.

"We're seeing it's easier to clone an invoice, create a supplier, fake a video call, fake an executive calling to authorize an invoice," a financial services audit leader at one roundtable said. "The voice spoofing is getting quite good."

A higher education audit leader in Minnesota said she doesn't feel fraud is any worse in her state than elsewhere around the country, "but it's just a real focus here. It's in the newspapers almost every day."

Another public sector auditor stated plainly, "We're getting a message from the federal government all the way down to our individual organizations: we need to prioritize fraud."

Exhibit 1.2. 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.

Geopolitical impacts

Geopolitical uncertainty remains one of the five highest risks after its rapid rise in the prior year (43%). In addition, on February 28, 2026, the U.S. and Israel initiated a joint attack against Iran, which led to Iran blockading maritime supply routes, volatile oil prices, and attacks against U.S. allies in the Middle East.

These geopolitical developments likely contributed to high supply chain risk for publicly traded (51%) and privately held (63%) organizations (Exhibit 1.3). In contrast, financial services, public sector, and nonprofit organizations report much lower geopolitical uncertainty risk (below 40%) (Exhibit 1.3).

Global politics are also having an impact on cybersecurity. More than 6 in 10 organizations said that geopolitically motivated cyberattacks – such as disruption of critical infrastructure or espionage – must be considered as part of their cybersecurity strategy, according a World Economic Forum survey. What's more, 91% of the largest organizations report changing their cybersecurity strategies because of geopolitical volatility.

Business resilience

Several audit leaders worried that the sharp decline in ranking for business resilience, down 17 percentage points year-over-year, could be misleading. The drop likely reflects choice displacement. What's more, some audit leaders noted that business resilience risk is absorbed into other higher ranked risks, such as cybersecurity and digital disruption. Still others noted that the pandemic and other disruptions in the past decade have tested and matured business continuity planning, making business resilience less novel. "We've lived it and survived it," one financial services audit leader said.

Notably, the public sector was higher in its ranking of business resilience than the North American average (42% vs. 29%) (Exhibit 1.3). This may reflect concerns about changing federal funding priorities and a shrinking federal workforce, which lost approximately 250,000 workers from December 2024 to January 2026, according to the U.S. Government Accountability Office (GAO).

Regulatory change

Another risk area that experienced displacement in North America was regulatory change, falling 9 percentage points and dropping to fifth place (Exhibit 1.2). This may be due to risk displacement from urgent emerging risks, accompanied by a trend toward deregulation from the current U.S. presidential administration.

Exhibit 1.3. North America – Top 5 Risks per Sector

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

Risk areas	All North America	Financial services	Publicly traded	Public sector	Privately held	Nonprofit
Cybersecurity	**85%**	**92%**	**85%**	**81%**	**88%**	**78%**
Digital disruption (including AI)	**69%**	**82%**	**76%**	**46%**	**58%**	**61%**
Human capital	**45%**	**49%**	42%	**54%**	**29%**	33%
Geopolitical/macroeconomic uncertainty	**43%**	37%	**61%**	25%	**63%**	28%
Regulatory change	**42%**	**44%**	37%	**48%**	21%	**67%**
Market changes/competition	41%	**51%**	**58%**	12%	**29%**	**50%**
Supply chain and outsourcing	33%	24%	**51%**	10%	**63%**	39%
Business resilience	29%	30%	17%	**42%**	**29%**	11%
Financial/liquidity	24%	25%	8%	37%	17%	**44%**
Fraud	18%	27%	8%	23%	17%	6%
Communications/reputation	16%	11%	8%	38%	4%	17%
Organizational culture	16%	10%	8%	25%	21%	33%
Governance/corporate reporting	14%	8%	10%	27%	17%	6%
Health/safety	11%	0%	7%	25%	17%	22%
Climate change/environment	7%	4%	10%	8%	17%	0%
Mergers/acquisitions	7%	7%	12%	0%	13%	6%

5 highest risks

Note 1: Ties for fifth place are highlighted in a lighter shade.
Note 2: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 232 for North America.

KEY POINTS

Survey insights

- Cybersecurity dominates risk rankings and holds first place, with 85% citing it as a Top 5 risk.
- Digital disruption risk rose significantly (+16) and is now ranked as the second highest risk.
- Geopolitical/macroeconomic uncertainty risk remains high, ranked fourth overall, with particularly high ratings among for-profit industries outside of financial services.
- Fraud risk increased by 7 percentage points in 2026 to 18%. Fraud risk rating has doubled since 2023.

Internal audit strategies

- Look for impacts from digital disruption and geopolitical uncertainty on other risk areas, including cybersecurity, business resilience, supply chain, third-party, and financial/liquidity.
- Expand thinking on supply chain risk to include software.
- Reassess third-party risk in an AI context and look for heightened vulnerabilities, particularly in data warehousing and cloud services.

2. INTERNAL AUDIT PRIORITIES

Audit Effort Focuses on Cybersecurity, Compliance, AI

Cybersecurity continues to dominate audit priorities, with 84% of respondents including it as a Top 5 area where internal audit spends the most time and effort, nearly matching its Top 5 risk score of 85%.

Regulatory change is ranked a distant second, with 54% saying it is a Top 5 audit priority. Digital disruption had the largest increase for audit priority out of all the audit areas – up 9 percentage points – bringing it to third in the ranking at 53%. Other areas where internal audit increased its efforts were fraud and human capital (+5) (Exhibits 2.1 and 2.2).

Cybersecurity efforts evolve

Cybersecurity is evolving. Instead of traditional perimeter-focused concerns, cybersecurity encompasses AI-enabled threats, software supply chain vulnerabilities, third-party ecosystems, cloud environments, cyber resilience, and increasingly sophisticated geopolitical cyberattack campaigns. This evolution supports a broader internal audit focus beyond traditional technical controls to areas such as cyber resilience, third-party ecosystems, AI-enabled security, and governance over emerging technologies.

AI effort continues to increase

Audit effort has continued to increase for digital disruption, reflecting persistent concerns about internal audit's ability to provide effective assurance over AI. Those listing it as a Top 5 audit priority have more than doubled (from 25% in 2023 to 53% in 2026). No other risk area remotely matches this acceleration (Exhibit 2.2). However, it's important to note that public sector functions are not included in this shift, with only 25% saying that digital disruption is one of their Top 5 audit priorities (Exhibit 2.3).

Although there is high audit priority for digital disruption in most sectors, the effort may reflect concern rather than confidence, according to roundtable participants.

"I think part of this might be that everyone thinks, 'Okay, I've got to do something in AI or this digital disruption space, or we're going to lose the company," one financial services audit leader said. "Internal auditors are saying, 'I need to go out there and audit something to help get us moving.'"

Shaun Kirby, who recently became CAE at Cumberland Farms and previously led the audit function at a semiconductor company, noted that effort considerations must include internal audit's use of AI in its work. He views AI as a tool that will shift audit from backward-looking to forward-looking through continuous monitoring. "What does that look like three to five years down the road?" he asked. "I wish I had a crystal ball."

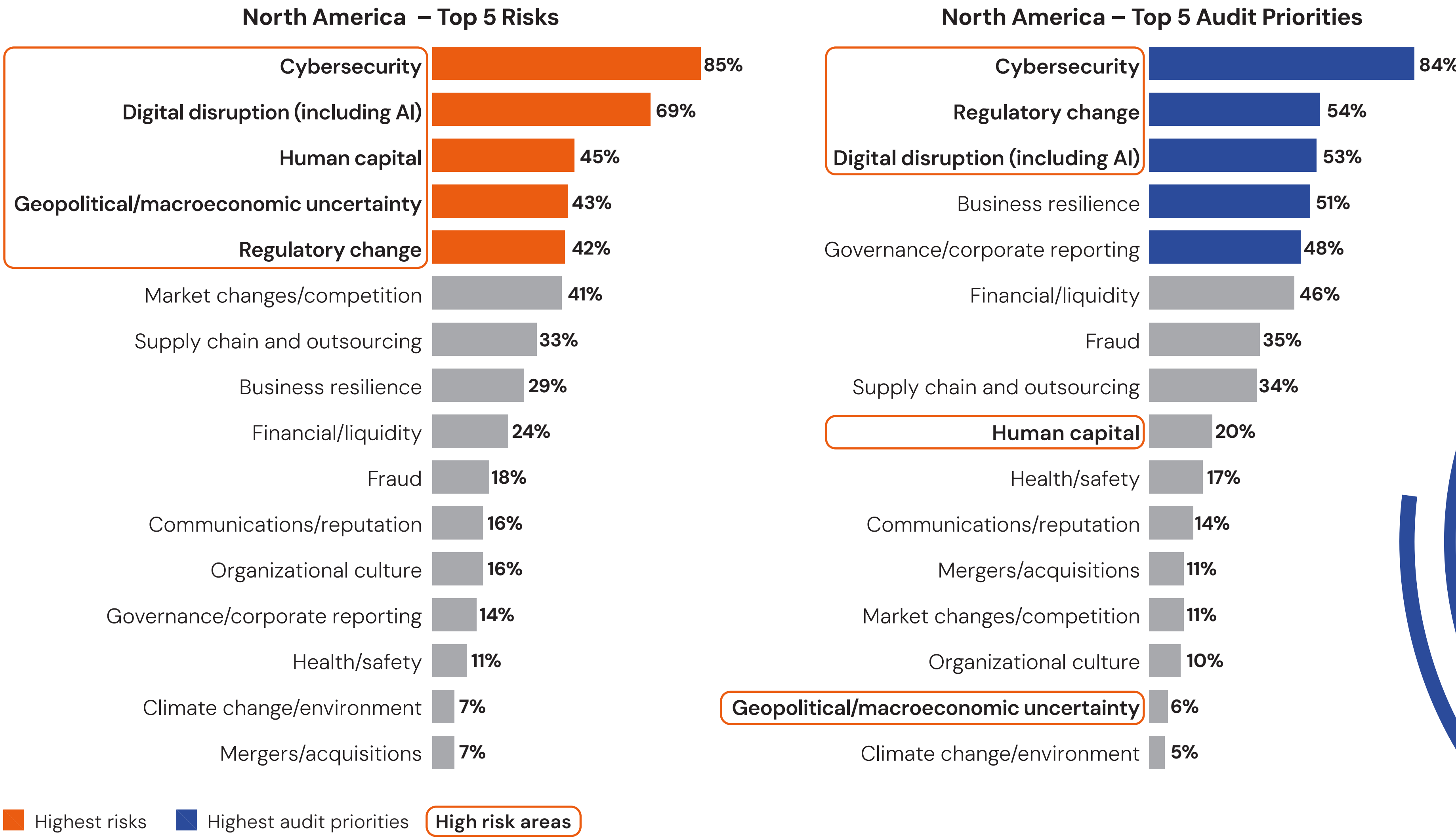
One private sector auditor offered an amusing but potentially prescient observation on the internal audit/AI relationship: "We have this phrase in our department," she said. "AI or IA? Who is watching who?"

"We have this phrase in our department. AI or IA? Who's watching who?"

– Roundtable comment

Exhibit 2.1. North America – 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* = 232 for North America.

Never-ending cybersecurity battles

Despite high effort toward cybersecurity, audit leaders worry they are falling behind, particularly given the influence of AI. Many simply don't have the resources or in-house expertise to keep up. Tremblay summed up the concern of audit leaders at the two roundtables: "To actually audit cybersecurity well would take an army, and an unfathomable budget, given the attack surface," he said.

Best practices in this area include prioritizing upskilling of audit staff, focusing on IT/cyber skills for new hires, and outsourcing. Another consideration is to work with IT and information security experts to leverage AI products to support cybersecurity by automating real-time threat detection, identifying network anomalies, and accelerating incident response. Governance best practices include ensuring that human oversight, security, and training regimens are part of any AI-enhanced cybersecurity strategy.

While it is important and necessary to build deeper skillsets within the audit function, internal auditors do not necessarily need to have the skills to fully perform first- or second-line cybersecurity. As noted in the Three Lines Model, internal audit's role is to provide assurance and advisory services.

Geopolitics and related efforts

While auditors focused their efforts primarily on cybersecurity, AI, and compliance, other highly ranked risk areas received less audit attention. As shown in Exhibit 2.1, there was a 30-percentage-point gap between risk ranking and audit priority for market changes/competition (41% vs. 11%). The gap was even greater (37 percentage points) for geopolitical/macroeconomic uncertainty (43% vs. 6%).

Roundtable participants said some gaps may be explained by the difficulty in directly auditing risk areas external to the organization, such as geopolitical uncertainty. However, its impact on internal risk areas can be monitored. Risk areas, including supply chain, financial/liquidity, and market changes/competition, can be influenced by wars, market instability, and international friction.

This was noted in supply chain audit priority ranking much higher than the regional average (34%) for publicly traded (51%) and privately held (71%) organizations, which are likely to rely more heavily on global resources to do business (Exhibit 2.3).

Additionally, audit coverage for some risks might be addressed in other risk areas. For example, financial/liquidity audit efforts could cover aspects of both market changes/competition and geopolitical uncertainty. Similarly, business resilience audit efforts could address aspects of geopolitical uncertainty.

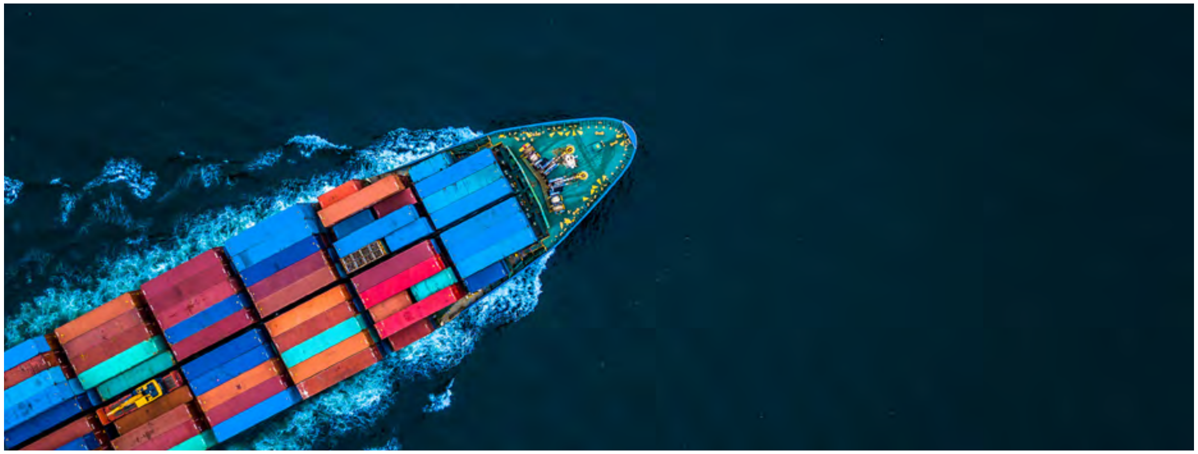


Exhibit 2.2. North America – Top 5 Audit Priorities Trend

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
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.

INTERNAL AUDIT PRIORITIES

Human capital and organizational culture

Human capital has consistently ranked low as an audit priority compared to risk level. While 45% of survey respondents listed it as a Top 5 risk, only 20% listed it as Top 5 for audit priority. The notable exception is public sector, where 44% listed human capital as a Top 5 audit priority (Exhibits 2.1 and 2.3).

Michael Callino, vice president of internal audit and automation at UPS, identified human capital as a risk area that should not be overlooked, particularly considering the influence of AI on strategic decisions on human capital. He described a trend where organizations are citing AI to justify job cuts, something referred to as "AI washing" by economists and media.

"You're seeing a lot of companies who make these decisions walking back on some of their cultural foundational elements," he said. "I think it's where the world is heading, and I think it's unfortunate."

Callino argues that the long-term impact on human capital risk can be significant for individual organizations because deteriorating culture could lead to talent flight. "If your culture starts to diminish, I think it has a bigger effect on the broader risk portfolio," he said.

Fraud

The increase in fraud risk ranking in the past four years has seen a commensurate increase in audit effort. Since 2023, the percentage of survey respondents identifying fraud as a Top 5 area for audit effort has increased from 26% to 35% (Exhibit 2.2). This may reflect previously cited concerns about AI's influence on fraud, as well as increasing pressure from federal regulators.

High effort toward compliance areas

Audit priority rankings for regulatory change (54%) and governance/corporate reporting (48%) reflect the profession's legacy orientation toward compliance auditing. Indeed, the difference between risk rankings and audit priorities was most stark for governance/corporate reporting. Just 14% of North American survey respondents ranked it as a Top 5 risk; yet 48% listed it as a top audit priority (Exhibit 2.1).

Richard Chambers, senior advisor for risk and audit at Optro (formerly AuditBoard), expressed concern over the heavy emphasis on regulatory change and corporate reporting in North American audit priorities. "We just cannot give up our quest to be compliance auditors," he said.

However, Chambers said agentic AI is poised to absorb much of the routine compliance and transaction-testing work that currently consumes much of internal audit's time and effort. "They are going to be able to identify the risks, select your samples, test them, identify the anomalies, and generate the audit results," he said. He stressed this change is an inevitable efficiency shift, not a distant possibility.

Human capital has consistently rated lower for audit priority (**20%**) than risk (**45%**), with the effects of AI adding another layer of dimension to the risk.

Exhibit 2.3. North America – Top 5 Audit Priorities per Sector

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

Audit areas	All North America	Financial services	Publicly traded	Privately held	Public sector	Nonprofit
Cybersecurity	**84%**	**92%**	**93%**	**67%**	**73%**	**89%**
Regulatory change	**54%**	**66%**	42%	**38%**	**60%**	**61%**
Digital disruption (including AI)	**53%**	**58%**	**64%**	**46%**	25%	**83%**
Business resilience	**51%**	**59%**	**46%**	**38%**	**54%**	**39%**
Governance/corporate reporting	**48%**	**56%**	**54%**	**38%**	**44%**	28%
Financial/liquidity	46%	52%	31%	**46%**	**50%**	**61%**
Fraud	35%	38%	36%	33%	38%	22%
Supply chain and outsourcing	34%	21%	**51%**	**71%**	21%	17%
Human capital	20%	11%	12%	25%	**44%**	6%
Health/safety	17%	3%	20%	21%	29%	22%
Communications/reputation	14%	13%	0%	8%	33%	11%
Mergers/acquisitions	11%	7%	20%	29%	0%	6%
Market changes/competition	11%	13%	8%	8%	4%	33%
Organizational culture	10%	6%	3%	13%	17%	22%
Geopolitical/macroeconomic uncertainty	6%	6%	7%	13%	6%	0%
Climate change/environment	5%	0%	12%	8%	2%	0%

5 highest audit priorities

Note 1: Ties for fifth place are highlighted in a lighter shade.
Note 2: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 232 for North America.

A CLOSER LOOK AT AI

Prepare Now for AI Audits

"AI-driven risks dominate the discussions I have with audit leaders," said Anthony Pugliese, IIA president and CEO.

Pugliese encourages internal auditors to focus on using their existing skills and judgment to start addressing AI risk. "They tell me, 'We just don't have the skillsets.' But we tell them if you just execute what you already know intuitively, you can move into auditing AI and AI governance."

Tremblay agreed: "I do think we are overstating how hard it is to audit AI. It's ones and zeros," he said. "It's a piece of software. While it feels new and novel, a good starting point is to treat it like any other piece of software, which we have been auditing for decades."

An audit leader from Canada said that internal auditors don't have the luxury of being neutral bystanders when it comes to establishing data governance practices related to AI. "There has to be some understanding of where the company is in that journey and really identifying it as a priority. Are we talking a hands-off approach, or is internal audit a real partner in this whole journey, advising them on a real-time basis of what controls or risks they need to look at?"

Callino stressed that auditing AI requires understanding "where it lives" in the organization. Using procurement data, vendor records and legal risk assessments, internal audit can build AI inventories, map regulatory exposure, assign risk owners, and create the foundational structure to make future auditing possible, he said.

KEY POINTS

Survey insights

- Cybersecurity continues to dominate audit priorities, with 84% of respondents including it as a Top 5.
- Digital disruption had the largest increase for audit priority out of all the audit areas – up 9 percentage points.
- Over a four-year period, audit priority for digital disruption more than doubled (from 25% in 2023 to 53% in 2026).
- Geopolitical uncertainty and human capital are both high for risk but low for audit priority.

Internal audit strategies

- Leverage AI tools to absorb routine compliance and transaction-testing work.
- Monitor the impact of external risks (such as geopolitical uncertainty) on internal risk areas, including supply chain, financial/liquidity, and market changes/competition.
- Ensure AI-enhanced cybersecurity strategies include human oversight, security, and ongoing training.
- Use procurement data, vendor records, and legal risk assessments to build AI inventories.

3. RISK MATURITY AND COVERAGE

Assessing Risk Governance Maturity and Audit Coverage

This year, for the first time, the Risk in Focus survey explored risk governance maturity and level of audit coverage. Of greatest concern are high-risk areas that fared poorly for both maturity and coverage – digital disruption and geopolitical uncertainty.

Risk governance maturity

Risk governance maturity reflects the extent to which risk management is embedded, formalized, and effective across the organization, making it a critical consideration for internal auditing, according to The IIA Global Practice Guide, Assessing the Risk Management Process.

Mature risk governance incorporates effective risk management practices and resilience into an organization's core strategy, culture, and daily operations. Financial/liquidity risk had the highest scores for both risk governance maturity (68%) and internal audit coverage (53%) (Exhibit 3.1).

Ideally, organizations would be able to build this level of maturity for all risks they face. However, new and emerging risks create a great challenge in this area.

Areas with low risk governance maturity

Two high-risk areas that fared poorly for both maturity and coverage were:

- Digital disruption(23% for governance maturity, 9% for audit coverage adequacy)
- Geopolitical uncertainty (31% for governance maturity, 15% for audit coverage adequacy) (Exhibit 3.1)

In contrast, maturity and coverage were stronger for risks that are well-understood and familiar, such as financial/liquidity (68% maturity, 53% coverage) and governance/corporate reporting (50% maturity, 39% coverage).

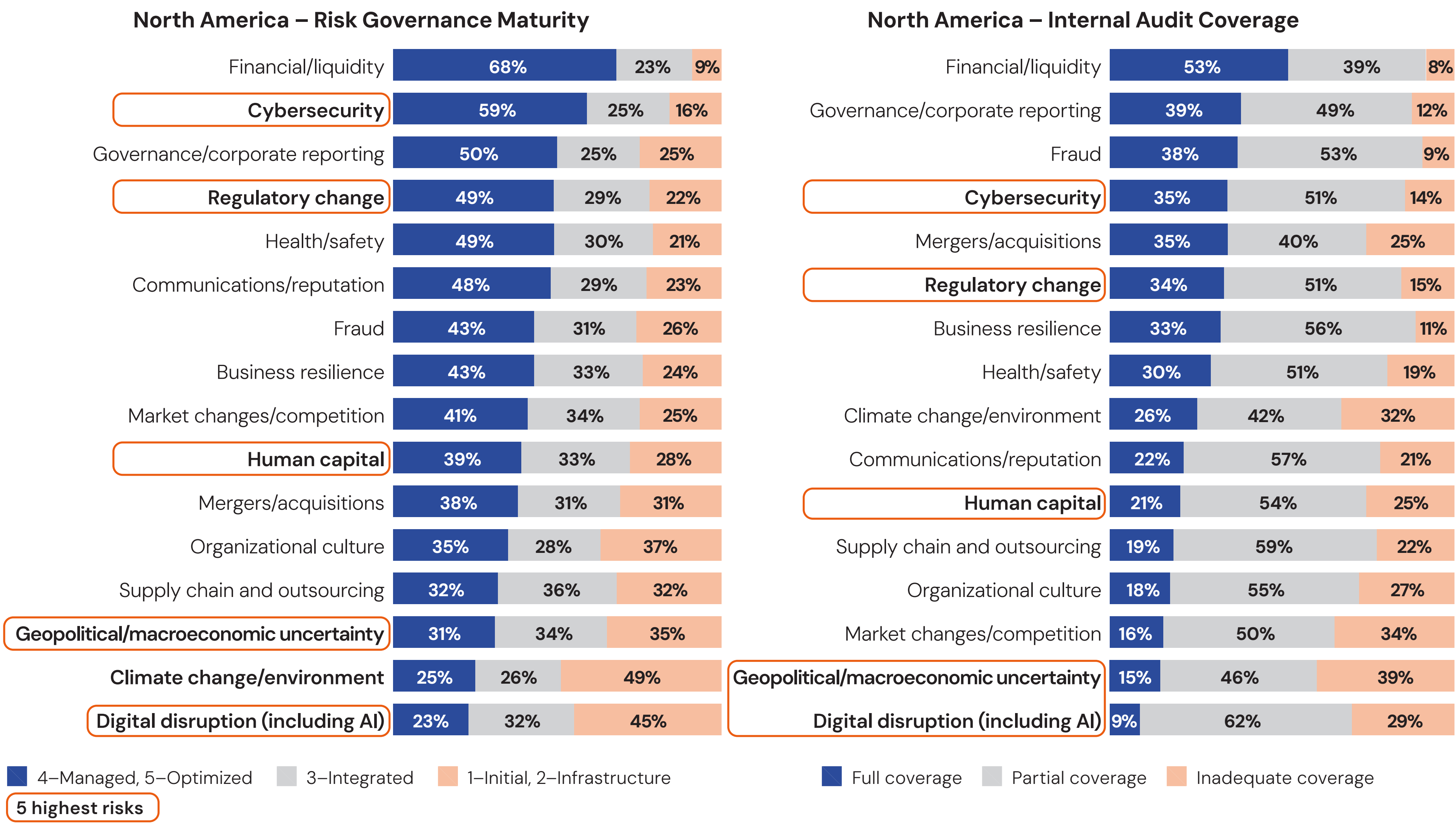
Some higher-risk areas showed middling maturity and coverage, such as human capital (39% maturity, 21% coverage) and market changes/competition (41% maturity, 16% coverage). One well-understood risk area that fared well in governance but less so in audit coverage was cybersecurity (59% maturity, 35% coverage).

Digital disruption had the lowest risk governance maturity, with only **23%** of CAEs scoring it as "managed" or "optimized."

RISK MATURITY AND COVERAGE

Exhibit 3.1. North America – 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.



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

RISK MATURITY AND COVERAGE

Concern over digital disruption maturity

Digital disruption ranked last in both risk governance maturity and audit coverage. Fewer than 1 in 4 (23%) respondents rated its governance as managed or optimized. Fewer than 1 in 10 (9%) reported full audit coverage (Exhibit 3.1). The wide gap between risk level and audit coverage is understandable, but not excusable, said Chambers.

"AI has proliferated and matured much faster than our ability to comprehend it and put the controls in place to assess the risk," he said. "If you have a risk that is exploding and your governance over it is proceeding at a snail's pace, then that accounts for why there's such a gap."

Building AI skills

Internal audit leaders face two concurrent challenges: the ongoing struggle to build relevant AI auditing skills, and the concentration of existing audit staff experience in other areas. Many audit functions are staffed heavily toward SOX and financial controls expertise, with limited bench strength in IT, cybersecurity, and emerging technologies. To build capacity, CAEs need to upskill existing staff and/or recruit technology talent from outside internal audit and teach them audit methodology.

Building risk governance maturity

For risks with low risk governance maturity, audit leaders may choose to shift the focus from assurance, which assesses past performance, to advisory, which focuses on the future.

Kirby suggests keeping the audit plan flexible to accommodate advisory requests throughout the year. In his previous CAE role, he tracked which audits were driven by management requests versus what was in the approved audit plan. In his last year at the job, 25% of work was management initiated, which he presented to the audit committee as a positive indicator of trust and relevance.

"When management is engaging us 25% of the time, that tells you what we're doing is value add," he said. "We're establishing a good relationship across the organization, and we're actually operating where the risk lives."

Callino and Kirby point out that communication with management is an essential aspect of building risk governance maturity in emerging risk areas. They expressed concern that in some cases internal auditors set risk levels in isolation, creating risk scores without management input, which can lead to internal audit functions focusing on the wrong things. Ultimately, risk governance maturity is a collaborative effort.

"If you have a risk that's exploding and your governance over it is proceeding at a snail's pace, that accounts for why there's such a gap [between risk and audit coverage]."

– Richard Chambers, senior advisor for risk and audit, Optro

KEY POINTS

Survey insights

- Of greatest concern are high-risk areas that fared poorly for both maturity and coverage – digital disruption and geopolitical uncertainty.
- Cybersecurity, while fairly high for risk governance maturity (59%) was relatively low for audit coverage (39%).
- Middling maturity was noted in other higher risk areas, including human capital and market changes/competition.
- Well-understood risks had the highest risk governance maturity and audit coverage, in particular, financial/liquidity and governance/corporate reporting.

Internal audit strategies

- Alert management/board to areas where risk management maturity and audit coverage are low, such as digital disruption, geopolitical uncertainty, and organizational culture.
- Leave space in audit plans to provide advisory services for areas where risk governance maturity is low.
- To increase audit skills for high-risk technology areas, upskill existing audit staff and/or recruit talent from outside internal audit, and teach them audit methodology.

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. Their responses provide a useful view of risk related to the organizations and industries where internal auditors work, but may not fully represent all types of risks or organizations in a geographical area.

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. North America – Industries per Sector

Publicly traded	
Manufacturing	27%
Mining, energy, and water supply	14%
Information and communication	14%
Wholesale and retail	10%
Health and social work	10%
Professional, scientific, technical activities	7%
Education	3%
Transport and storage	3%
Real estate	3%
Arts, entertainment, and recreation	3%
Administrative and support services	2%
Construction	2%
Accommodation and food services	2%

Privately held	
Manufacturing	29%
Transport and storage	21%
Mining, energy, and water supply	17%
Arts, entertainment, and recreation	13%
Agriculture, forestry, and fishing	8%
Information and communication	4%
Wholesale and retail	4%
Real estate	4%

Nonprofit	
Health and social work	44%
Education	28%
Mining, energy, and water supply	6%
Arts, entertainment, and recreation	6%
Real estate	6%
Public sector (including government)	5%
Professional, scientific, technical activities	5%

Public sector	
Public sector (including government)	52%
Education	27%
Mining, energy, and water supply	6%
Health and social work	4%
Transport and storage	4%
Administrative and support services	2%
Construction	2%
Agriculture, forestry, and fishing	2%
Other	1%

Financial services	
Financial and insurance activities including banking, investment, insurance	100%

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

APPENDIX C. GLOBAL RISK OVERVIEW

Digital Disruption and Geopolitical Risks Rising Rapidly

Disruption, both digital and geopolitical, defined the global risk landscape in 2026, driven by AI's pervasive impacts and rising instability fueled by wars in Ukraine and the Middle East.

Cybersecurity maintained the number 1 position, listed as a Top 5 risk by 80% of respondents (Exhibit C.1). Compared to the prior year, cybersecurity risks rose the most for Africa (+11), Asia Pacific (+10), and the Middle East (+9).

Keeping its second place ranking from last year, digital disruption rose 10 percentage points overall, largely driven by Asia Pacific (+20) and North America (+16).

Geopolitical uncertainty risk rose from sixth to third in the global risk rankings, increasing by 10 percentage points. The most dramatic increase was for the Middle East, 31 percentage points, followed by Asia Pacific (+13). Nearly half (48%) of respondents listed geopolitical uncertainty as a Top 5 risk, compared to only 30% in 2023.

Although not reaching the top of the risk ratings, it's notable that fraud risk ratings rose 6 percentage points globally.

As technology and geopolitical risks rose, they displaced business resilience (–12) and regulatory change (–9) in the risk rankings.

Regional risks – convergence and hot spots

Across regions, the highest ranked risks are becoming more similar, creating key areas of risk convergence around technology and geopolitical uncertainty (Exhibit C.2).

Cybersecurity is the highest ranked risk for every region, and digital disruption takes second place for all but one region. Geopolitical uncertainty was in the Top 5 for all regions for the first time since the survey started four years ago, taking third place for most.

Even with risk convergence in key areas, systemic differences expose each region to unique risks (Exhibit C.1).

- **Africa:** Africa faces greater challenges with fraud (50%) and financial/liquidity (49%) compared to other global regions. Notably, risk levels rose moderately across a wide range of risk areas, as risk ratings for business resilience decreased substantially (–21).
- **Asia Pacific:** Asia Pacific rated risk levels higher than average for business resilience (43%), market changes (37%), and supply chain (33%). The region saw a significant reshuffling of risk rankings compared to the prior year.
- **Europe:** Similar to the previous year, regulatory change (40%) ranked high for the region and well above the global average (32%). Human capital risk was in the Top 5 (39%).
- **Latin America:** Latin America saw higher risk rankings for fraud (38%) compared to the global average.
- **Middle East:** Business resilience (47%) and financial/ liquidity risks (42%) were higher in the Middle East.
- **North America:** Compared to the average of the regions, risk ratings for North America were higher for market changes/competition (41%), regulatory change (42%), human capital (45%), and supply chain (33%) (Exhibit C.2).

MORE GLOBAL RESOURCES

See the ***Risk in Focus Global Summary report*** for regional trend data and analysis.

Exhibit C.1. 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.

Exhibit C.2. 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 (including third parties)
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

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**

REPORT SPONSOR

Optro (formerly AuditBoard) is the leading AI-powered GRC platform transforming enterprise risk into opportunity. More than 50% of the Fortune 500 trust Optro to elevate their GRC teams and see risk before it happens. Optro is top-rated by customers on G2 and Gartner Peer Insights, and was named a Leader in the 2025 Gartner® Magic Quadrant™ for Governance, Risk and Compliance (GRC) Tools, Assurance Leaders, and was also named to the Deloitte Technology Fast 500™ for the seventh consecutive year. To learn more, visit optro.ai.

Optro

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.

Internal Audit FOUNDATION 1976-2026

Research Team

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

Project manager
Candace Sacher

Roundtable moderator
Brian Tremblay, CIA

Writer
Robert Perez

Graphic designers
Sergio Analco and
Cathy Watanabe

INTERNAL AUDIT FOUNDATION PARTNERS

DIAMOND PARTNERS

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.

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

BACK

CONTENTS