RISK in FOCUS

LATIN AMERICA 2026/2027

Hot Topics for Internal Auditors

Fundación Latinoamericana de Auditores Internos

50 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.

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

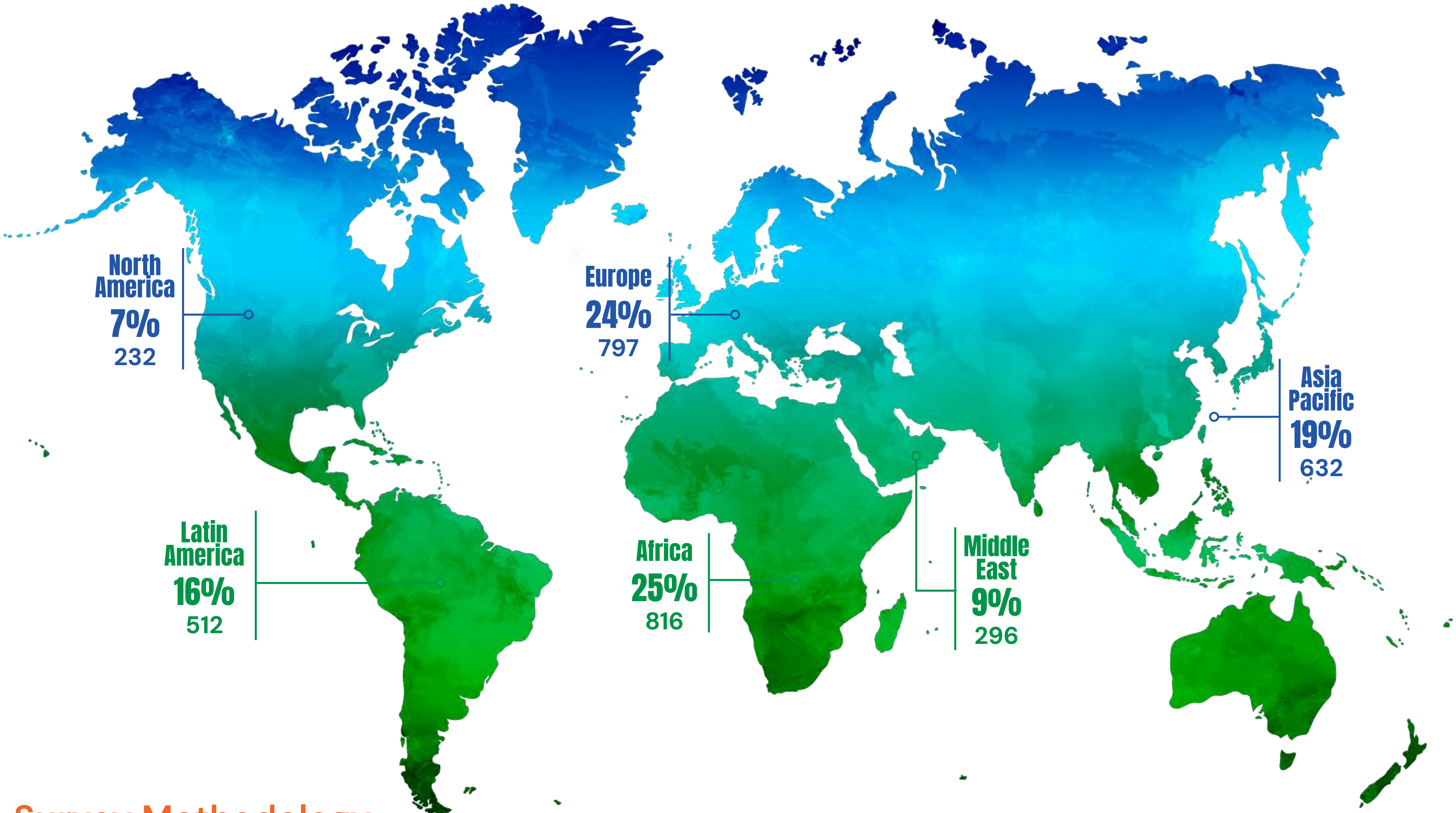
12 in-depth interviews

GLOBAL SURVEY PARTICIPATION

GLOBAL TOTALS

3,285 respondents

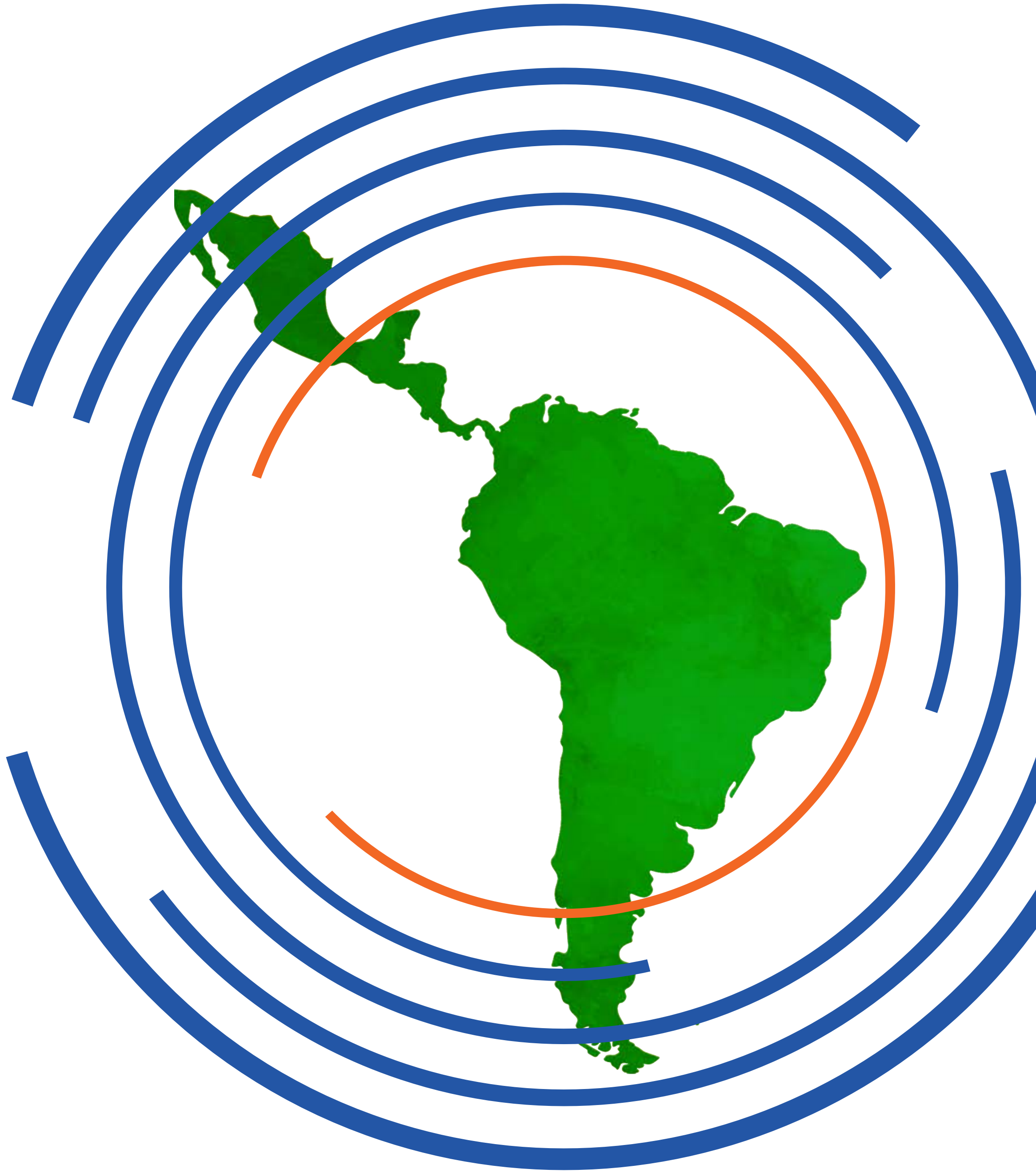
132 countries/locations



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 Awareness to Strategic Audit Action

Latin America's risk environment is no longer defined by isolated threats. Cybersecurity, digital disruption, geopolitical uncertainty, fraud, talent, regulation, and liquidity now operate as an interconnected risk system. The challenge for chief audit executives is to convert awareness into audit coverage, advisory insight, and board-level action.

Latin America's 2026/2027 Risk in Focus results show a region facing a more digital, volatile, and interconnected risk landscape. Cybersecurity remains the dominant concern, selected by 80% of respondents as a Top 5 risk and rated as high by 82%.

However, the more important story is the speed and breadth of change around it.

Digital disruption, including artificial intelligence, is now the second-highest Top 5 risk at 61%, while 75% rated it as high. Geopolitical/macroeconomic uncertainty follows closely, selected as a Top 5 risk by 52% and rated high by 71%.

Five findings stand out from this research:

- Cybersecurity has become a business resilience and trust issue. Roundtable participants described cyber risk not only as a technology risk, but also as a risk to operations, critical infrastructure, customer confidence, reputation, regulatory compliance, and recovery capability.
- Digital disruption is accelerating faster than governance. AI, automation, bots, low-code tools, cloud services, and data analytics are changing business processes faster than many organizations can update controls, policies, skills, and accountability structures.
- Geopolitical and macroeconomic uncertainty must be translated into audit-relevant impacts. For Latin America, this risk appears through supply chains, foreign exchange, fuel prices, cloud location, regulatory change, cross-border operations, public infrastructure, and business continuity.
- Internal audit priorities remain more traditional than the risk landscape. Cybersecurity, fraud, financial/liquidity, regulatory change, and digital disruption are the five highest audit priorities. However, significant gaps remain for geopolitical/macroeconomic uncertainty, market changes, climate/environment, human capital, culture, and digital disruption relative to risk level and governance maturity.
- Maturity and coverage are the next frontier. Digital disruption has the lowest level of risk governance maturity, yet it is one of the highest risks. It also has the lowest level of full internal audit coverage. This mismatch is a call to action for CAEs.

The main message for chief audit executives is clear: the profession cannot rely only on familiar audit programs and legacy risk categories. CAEs must help boards and executive teams understand how emerging risks connect to strategy, operations, people, technology, fraud, regulation, and resilience. In 2027, leading internal audit functions will not be defined by the number of audits completed, but by their ability to focus scarce resources on the risks that could most affect organizational value.

LATIN AMERICA RESEARCH PARTICIPATION

512 survey responses

18 countries/locations

2 roundtables with **23** participants

4 in-depth interviews

REPORT AUTHOR

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

RESEARCH PARTNER

Fundación Latinoamericana **de Auditores Internos**

1. RISK ENVIRONMENT

A More Connected and Less Forgiving Risk Landscape

The 2026/2027 Risk in Focus results for Latin America show a clear concentration of concern around three risks: cybersecurity, digital disruption, and geopolitical/macroeconomic uncertainty.

These risks are not new, but the conversations with audit leaders across the region suggest that their drivers have changed. Cybersecurity is no longer viewed as an IT risk alone. Digital disruption is no longer limited to technology strategy. Geopolitical uncertainty is no longer a distant external risk. Each now has direct implications for operations, governance, resilience, compliance, fraud, reputation, and talent.

Cybersecurity risk

As shown in Exhibit 1.1, cybersecurity is the highest risk by a wide margin. It was chosen as a Top 5 risk by 80% of respondents and rated as high by 82%. This confirms that cyber remains the defining risk for boards, management, and internal audit in the region. Roundtable participants described a risk environment where cyber threats are becoming more sophisticated, more frequent, and more closely tied to fraud, identity, data protection, operational technology, and business continuity. AI can improve defense, but it also improves attack capability. Fraudsters can automate phishing, create synthetic identities, imitate voices, generate realistic messages, and exploit vulnerabilities faster.

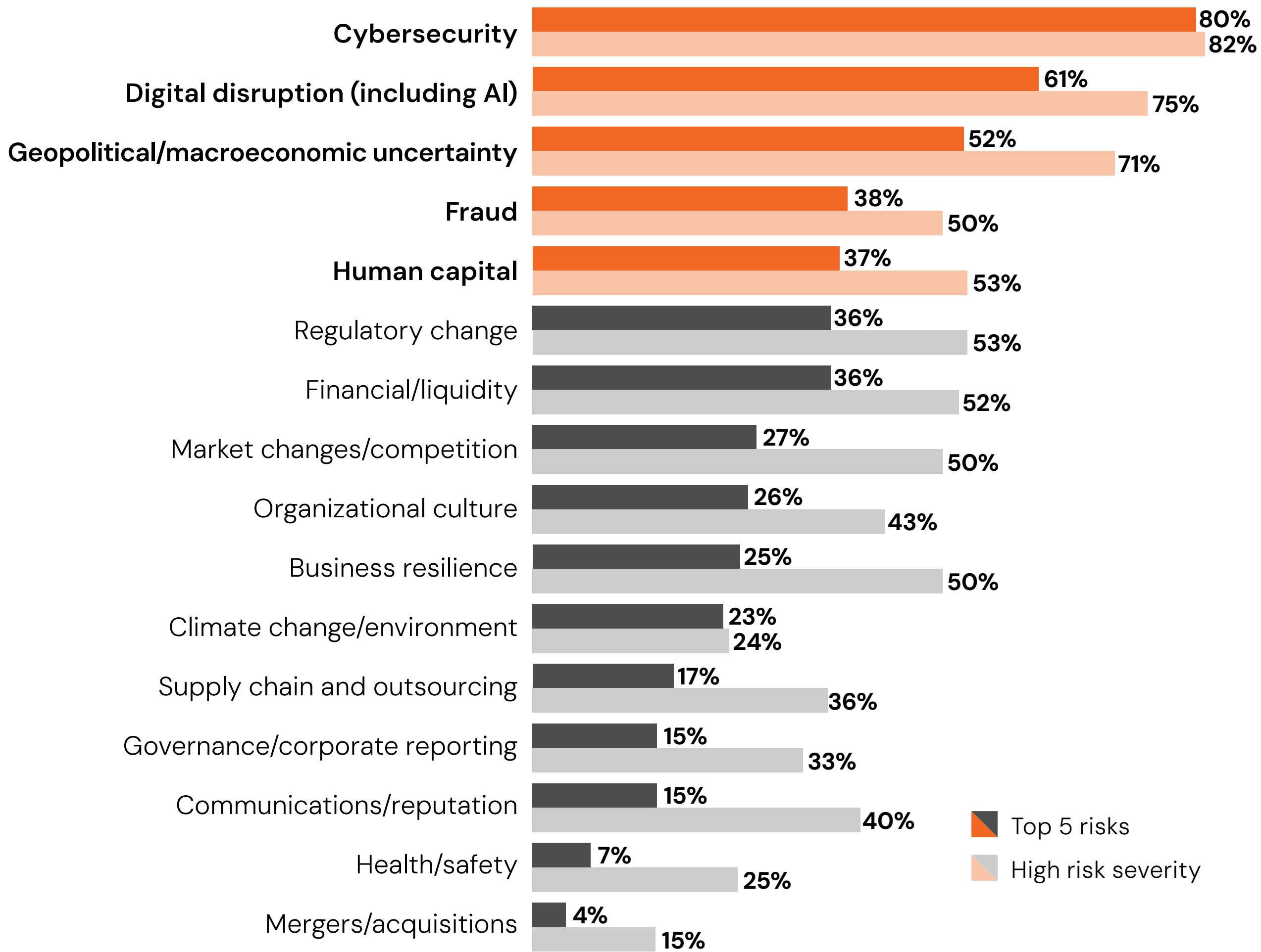
For many organizations, the cyber risk perimeter has expanded. It now includes cloud environments, outsourced technology providers, industrial automation, digital channels, mobile applications, remote access, data lakes, artificial intelligence tools, and operational technology.

At the same time, cybersecurity risk considerations need to go beyond traditional information technology operations. For example, one roundtable participant described the challenge of cybersecurity for highly automated industrial operations, where production technology had evolved over many years, but security controls had not kept the same pace. This is an important signal for CAEs: cyber risk should not be assessed only through corporate IT. It must also be assessed through operations, third parties, digital products, customer channels, and critical infrastructure.

Cybersecurity continued to dominate the risk rankings, with **80%** of CAEs in Latin America scoring it as one of their Top 5 risks.

Exhibit 1.1. Latin 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* = 512 for Latin America.

RISK ENVIRONMENT

Digital disruption risk

Digital disruption, including AI, is the second-highest Top 5 risk, selected by 61% of respondents and rated as high by 75%. In addition, digital disruption risk increased substantially compared to the prior year (Exhibit 1.2). This may be the most important movement in the Latin American risk landscape.

The opportunities created by AI are significant: automation, productivity, analytics, customer experience, fraud detection, and decision support. But the risk is equally significant: inaccurate outputs, biased models, data leakage, cyber vulnerabilities, shadow AI, regulatory breaches, intellectual property exposure, and unclear accountability.

The issue is not whether organizations should adopt new technologies. In many sectors, the competitive pressure to adopt AI and digital tools is already unavoidable. The issue is whether organizations can adopt them with enough governance, accountability, transparency, resilience, and control. Interviewees noted that executives increasingly recognize digital transformation as important, but day-to-day operational pressures often delay action. This creates a gap between risk awareness and risk response.

The maturity of organizational governance for AI varies. Some organizations are creating AI committees, governance models, policies, approval processes, and data controls. Others are still discovering that business units have already adopted AI tools without formal governance. For internal audit, the global rise in AI means that audit methodologies must evolve quickly. Auditors need criteria to evaluate AI governance, but also practical ways to test controls around data, access, monitoring, vendor management, model outputs, and human oversight.

Geopolitical uncertainty risk

Geopolitical/macroeconomic uncertainty ranks third, selected by 52% as a Top 5 risk and rated high by 71%. Compared to last year, geopolitical uncertainty risk increased substantially, likely due in part to the conflict that started on February 28, 2026, when the U.S. and Israel initiated a joint attack against Iran. Geopolitical uncertainty tied digital disruption as one of the two fastest growing risks in the region (Exhibit 1.2).

In prior years, geopolitical uncertainty was often discussed as a broad external risk. This year, the discussions were more practical and specific. Geopolitical risk in Latin America should be viewed through both external and domestic lenses. External drivers include trade policy, tariffs, armed conflicts, cross-border regulation, commodity prices, and global technology dependencies. Domestic drivers include election cycles, institutional stability, economic policy shifts, fiscal decisions, social unrest, and changes in the role of the state in the economy. Both types of drivers can affect interest rates, investment appetite, liquidity, foreign exchange, regulatory agendas, and operating continuity. In other words, geopolitical risk becomes audit-relevant when it is translated into specific business impacts.

"The most relevant risks in Latin America are no longer isolated. Cyber, AI, fraud, liquidity, talent, and geopolitics are now part of the same risk conversation."

– Renato Trisciuzzi, Brazil

Exhibit 1.2. 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.

In the airline sector, geopolitical uncertainty can affect routes, airport access, regulatory permissions, fuel prices, taxes, and passenger demand. In financial services, it can affect liquidity, credit risk, fraud, cyberattacks, regulation, and customer behavior. In health and insurance, it can affect medicines, medical supplies, equipment, logistics, and continuity plans. In public sector and critical infrastructure, it can affect service delivery, national resilience, public trust, and response capability.

Roundtable participants emphasized that geopolitical risk is often felt through operational consequences. These consequences differ by sector, but the CAE's role is similar: help management and the board understand scenarios, dependencies, trigger points, and response plans.

Fraud risk

Fraud was selected as a Top 5 risk by 38% and rated high by 50%. This result should be read together with cybersecurity, digital disruption, macroeconomic pressure, and human capital.

Fraud risk is increasingly enabled by digital channels, identity manipulation, social engineering, cyber breaches, economic stress, third parties, and weak data governance. The growth of AI also introduces new fraud scenarios, including synthetic identities, deepfakes, automated phishing, prompt manipulation, and faster exploitation of vulnerabilities. The boundary between cyber risk and fraud risk is becoming less clear. For CAEs, this means cyber and fraud audit plans should be coordinated. Digital identity, access management, transaction monitoring, incident response, and customer communication should be assessed together.

Fraud risk in Latin America also has a strong relationship with financial/liquidity risk and macroeconomic pressure. Economic volatility can increase incentives and opportunities for fraud. Liquidity stress can weaken control discipline. Inflation can change procurement behavior, inventory risk, pricing decisions, and customer credit quality. Public sector organizations may face additional pressure around transparency, service continuity, and public trust.

Human capital, regulatory change, financial/liquidity risk

Human capital, regulatory change, and financial/liquidity risk form the next layer of concern. Human capital was selected as a Top 5 risk by 37% and rated high by 53%. Regulatory change was selected as Top 5 by 36% and rated high by 53%. Financial/liquidity risk was selected as Top 5 by 36% and rated high by 52%. Human capital should also be viewed through a geopolitical and macroeconomic lens. In developing economies, highly qualified professionals in cybersecurity, data, automation, artificial intelligence, finance, and risk management may have opportunities in larger global markets or through remote work for organizations outside the region. This movement can deepen capability gaps for Latin American organizations. For CEOs and boards, brain drain is not only an HR issue; it can affect transformation execution, cyber resilience, compliance, innovation, and internal audit capability.

A complicated risk network

These results show that the region is not moving from "old risks" to "new risks." Instead, traditional and emerging risks are becoming more connected, creating a complicated risk network, with implications for the organization as a whole. Digital disruption requires new talent. Cybersecurity requires investment. Geopolitical uncertainty can trigger regulatory changes. Financial stress can increase fraud. Talent gaps can limit the organization's ability to transform.

Exhibit 1.3. Latin America – Top 5 Risks per Sector

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

Risk areas	All Latin America	Financial services	Public sector	Privately held	Publicly traded
Cybersecurity	**80%**	**88%**	**70%**	**78%**	**79%**
Digital disruption (including AI)	**61%**	**74%**	43%	**62%**	**55%**
Geopolitical/macroeconomic uncertainty	**52%**	**52%**	40%	**53%**	**69%**
Fraud	**38%**	41%	**46%**	32%	33%
Human capital	**37%**	32%	**46%**	**39%**	36%
Regulatory change	36%	**43%**	**47%**	29%	19%
Financial/liquidity	36%	**42%**	21%	35%	**38%**
Market changes/competition	27%	24%	11%	**37%**	**38%**
Organizational culture	26%	17%	**46%**	27%	12%
Business resilience	25%	28%	23%	23%	26%
Climate change/environment	23%	20%	21%	27%	26%
Supply chain and outsourcing	17%	13%	10%	23%	33%
Governance/corporate reporting	15%	10%	32%	11%	12%
Communications/reputation	15%	12%	28%	11%	10%
Health/safety	7%	2%	7%	11%	10%
Mergers/acquisitions	4%	2%	10%	3%	5%

5 highest risks

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

RISK ENVIRONMENT

Sector differences

Sector differences are an important factor in understanding an organization's "risk network," as shown in Exhibit 1.3.

- Across sectors, cybersecurity remains a common risk, but the exposure differs. In financial services, cybersecurity and digital disruption are closely connected to digital identity, fraud, data security, customer trust, resilience, and regulatory expectations. However, operational technology (OT) cybersecurity is becoming increasingly relevant in manufacturing, food and beverage, pulp and paper, mining, energy, oil and gas, utilities, and other industrial environments, where a cyber incident can interrupt production, compromise safety, affect critical infrastructure, or disrupt service delivery.
- In publicly traded companies, geopolitical/ macroeconomic uncertainty and market changes are more prominent.
- In privately held companies, digital disruption, macroeconomic uncertainty, human capital, and market competition appear as significant strategic concerns.
- In the public sector, the risk profile is spread across a wide range of risk areas, led by cybersecurity, regulatory change, fraud, and human capital, but risk is also high for digital disruption, geopolitical uncertainty, and governance.

Climate change/environment risks

Climate change/environment is selected as a Top 5 risk by 23%, and only 24% rated it as high. This relatively low regional ranking should be interpreted carefully. In many Latin American organizations, climate and environmental risk compete with more immediate pressures, including economic growth, inflation, liquidity, security, infrastructure, employment, and regulatory change. Exposure also varies significantly by country, geography, and sector. For some sectors, such as energy, agriculture, transport, public infrastructure, insurance, mining, manufacturing, and government, climate and environmental risk can be severe. However, in other organizations, the risk may not yet be fully translated into operational, financial, compliance, insurance, asset protection, supply chain, or resilience impacts. For CAEs, the key question is not whether climate risk is high for all organizations, but whether it is properly assessed where exposure is significant.

Communications/reputation risks

Communications/reputation is selected as a Top 5 risk by only 15% but rated high by 40%. This gap deserves attention. Reputation may not always appear as a standalone audit universe category, but it is often the consequence of failures in cyber, fraud, safety, customer experience, regulation, ethics, ESG, and operational continuity. For digital banks, fintechs, airlines, public services, and consumer businesses, reputational damage can materialize quickly and spread through social media before management has time to respond.

Summary

The overall trend is clear: Latin America's risk environment is moving from single-risk management to connected-risk management. The highest risks should not be audited as separate silos. Cybersecurity, AI, fraud, talent, third parties, liquidity, regulation, continuity, and reputation must be assessed together, because the events that cause the greatest damage often combine several of these risks.

Latin America's risk environment is moving from single-risk management to connected-risk management.

KEY POINTS

Survey insights

- Cybersecurity remains the leading risk in Latin America, but the broader trend is the convergence of technology, macroeconomic uncertainty, fraud, regulation, and human capital.
- Digital disruption and AI are becoming high-risk areas because adoption is moving faster than governance.
- Geopolitical/macroeconomic uncertainty is high because it is no longer abstract; it affects supply chains, cloud strategy, foreign exchange, fuel, liquidity, regulation, and continuity.

Internal audit strategies

- CAEs should update the audit universe to reflect connected risks rather than isolated categories.
- Cybersecurity audits should include cloud, third parties, operational technology, data protection, resilience, and incident recovery.
- Digital disruption should be assessed through AI governance, data quality, model risk, automation controls, ethical use, and accountability.
- Geopolitical risk should be translated into auditable scenarios such as supply disruption, liquidity stress, regulatory change, foreign exchange exposure, critical infrastructure dependency, and business continuity.

2. INTERNAL AUDIT PRIORITIES

The Coverage Gap: When Risk Moves Faster Than Audit Plans

The survey results for internal audit priorities show that CAEs in Latin America are responding to the risk landscape, but not always at the same speed or with the same intensity as risk levels are changing.

Exhibit 2.1 shows that cybersecurity is both the highest risk and the highest audit priority. It was selected as a Top 5 audit priority by 74% of respondents. This alignment is appropriate and expected. However, the more important insight is found in the gaps between high-risk areas and lower levels of internal audit effort.

Fraud, financial/liquidity, regulatory change, and digital disruption complete the five highest audit priorities in Latin America. Fraud was selected as a Top 5 audit priority by 56%, financial/liquidity by 53%, regulatory change by 53%, and digital disruption by 47%. These results show that internal audit functions continue to devote significant effort to risks that are familiar, measurable, regulated, and traditionally within the internal audit comfort zone.

Digital disruption audit priority

The growth of digital disruption as an audit priority is encouraging, showing the most increase in effort for any audit area in the survey (Exhibit 2.2). However, its priority remains below its risk level. Digital disruption was selected as a Top 5 risk by 61%, but as an audit priority by 47%. The gap becomes even sharper when viewed alongside maturity and coverage data in Section 3.

Digital disruption is one of the highest risks, but one of the lowest areas for mature governance and full audit coverage. This is one of the most important findings of the report.

Roundtable participants and interviewees offered several explanations. First, some organizations recognize digital disruption as strategically important, but operational pressures dominate daily decision-making. In retail, for example, executives must continue to manage sales, cash, logistics, shrinkage, margins, and customer experience while also transforming processes and technology. As Magy Fuentes described, the challenge is to "perform and transform" at the same time.

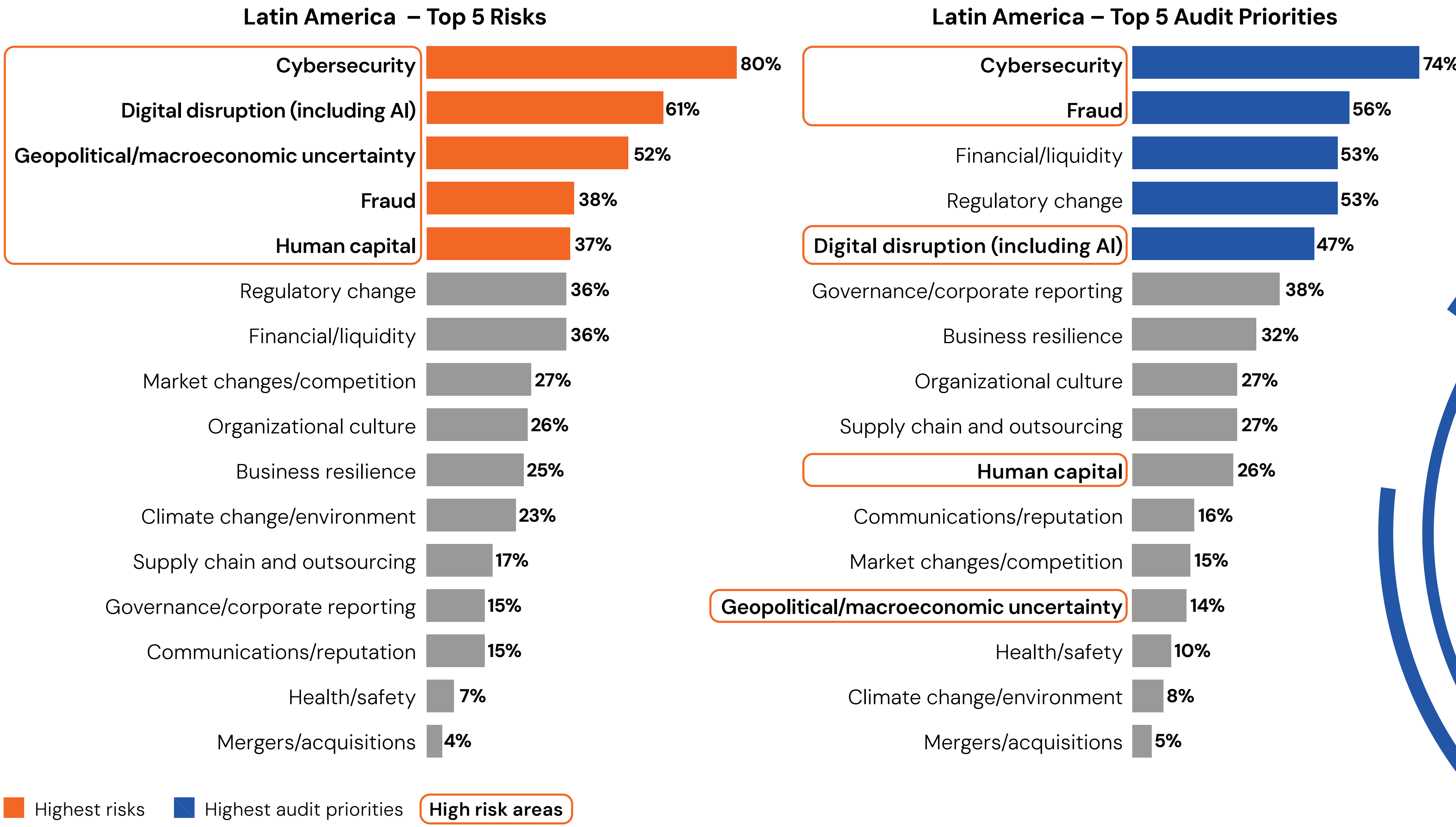
Digital disruption scored high for risk (**61%**), but relatively low for audit priority (**47%**). Plus, it is one of the lowest areas for mature governance and full audit coverage.

"Digital transformation and cybersecurity are clearly recognized as relevant. The challenge is that, in many organizations, they are still more of a concern than an occupation."

– Magy Fuentes, Argentina

Exhibit 2.1. Latin 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* = 512 for Latin America.

Second, some internal audit teams lack the competencies needed to audit AI, cloud, automation, data governance, algorithms, cybersecurity, operational technology, or digital products. This is not only a staffing issue. It is also a methodology issue. Traditional audit programs may not be sufficient for evaluating agile development, machine learning models, bots, AI agents, data lineage, digital identity, cloud resilience, or platform ecosystems. CAEs should consider building or maintaining multidisciplinary capabilities within the internal audit function, including information technology, cybersecurity, automation, data analytics, artificial intelligence, operational technology, process, and business expertise. Where permanent staffing is not feasible, standing co-sourcing arrangements or access to specialized subject matter experts may be necessary. Even under pressure to perform traditional audits, CAEs should reserve dedicated space in the annual audit plan for emerging risks through targeted assurance, readiness assessments, advisory reviews, continuous monitoring, or pilot audits.

Third, some CAEs may remain too close to what is familiar. Interviewees were candid about the profession's comfort zone. Auditing finance, compliance, procurement, payroll, or regulatory reporting can be more straightforward because criteria are clearer and teams have experience. Auditing culture, innovation, digital transformation, geopolitical exposure, or strategic resilience requires more judgment, more collaboration, and more willingness to engage with ambiguity.

Geopolitical uncertainty audit priority

Geopolitical/macroeconomic uncertainty presents the largest gap between risk and audit priority. It was selected as a Top 5 risk by 52%, but only 14% selected it as a Top 5 audit priority. At first glance, this may look like under-coverage. In practice, the issue is more nuanced. Geopolitical risk is difficult to audit directly. Internal audit cannot audit a war, an election, inflation, diplomatic conflict, or commodity market volatility. However, internal audit can audit how the organization anticipates, monitors, escalates, and responds to the impact of these conditions in the external risk environment.

This means CAEs should not necessarily create an audit called "geopolitical risk." Instead, they can incorporate geopolitical and macroeconomic scenarios into existing audit areas within the organization, such as supply chain, liquidity, treasury, strategic planning, business continuity, regulatory compliance, third-party risk, cloud concentration, crisis management, and market expansion. For example, a fintech may translate geopolitical risk into cloud dependency and recovery strategy. An airline may translate it into airport access, route permissions, foreign exchange exposure, and fuel prices. A healthcare or insurance organization may translate it into medical supply continuity.

"Geopolitical risk becomes real when it affects medicines, medical supplies, equipment, logistics, and operational continuity."

– José Luis Fernández García, Chile

Exhibit 2.2. Latin 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
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.

INTERNAL AUDIT PRIORITIES

Human capital audit priority

Human capital is another area with a significant gap. It was selected as a Top 5 risk by 37%, but only 26% selected it as a Top 5 audit priority. This is understandable, because human capital can be difficult to audit beyond traditional HR processes. However, the interviews suggest that talent is a risk enabler across almost all other risks. Without the right talent, organizations cannot govern AI, protect against cyber threats, execute transformation, maintain controls, respond to regulation, detect fraud, or build resilient operations.

Internal audit should therefore expand its view of human capital. It is not only about turnover, recruitment, training, or succession. It is also about strategic capability. Does the organization have the skills needed to execute its strategy? Are critical roles identified? Are digital, cyber, data, and risk capabilities sufficient? Are knowledge transfer and succession plans effective? Are incentives aligned with ethical behavior and prudent risk-taking? Are culture and leadership behaviors supporting risk awareness?

Market changes/competition audit priority

Market changes/competition is selected as a Top 5 risk by 27%, but only 15% selected it as a Top 5 audit priority. This gap may reflect another traditional limitation: internal audit often focuses more on internal processes than external market dynamics. However, market risk can affect pricing, customer behavior, credit quality, inventory, product design, digital channels, liquidity, and strategy execution. CAEs should consider whether market changes are incorporated into strategic risk assessments and whether management has effective mechanisms to monitor and respond.

Climate change/environment audit priority

Climate change/environment has a similar pattern. It was selected as a Top 5 risk by 23%, but only 8% selected it as an audit priority. For many organizations, this may be appropriate if exposure is low. But for organizations in agriculture, energy, mining, transport, insurance, infrastructure, public sector, and manufacturing, the low audit priority may indicate a need to reassess. Climate risk should be evaluated not only as sustainability reporting, but as operational resilience, asset protection, supply chain disruption, regulation, insurance cost, and community impact.

Exhibit 2.3. Latin 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 Latin America	Financial services	Public sector	Privately held	Publicly traded
Cybersecurity	**74%**	**88%**	**52%**	**68%**	**83%**
Fraud	**56%**	**55%**	46%	**65%**	**55%**
Financial/liquidity	**53%**	**65%**	34%	**52%**	**38%**
Regulatory change	**53%**	**61%**	**62%**	**44%**	29%
Digital disruption (including AI)	**47%**	**58%**	38%	**42%**	**48%**
Governance/corporate reporting	38%	34%	**51%**	32%	**38%**
Business resilience	32%	32%	26%	35%	**38%**
Organizational culture	27%	15%	**47%**	25%	26%
Supply chain and outsourcing	27%	15%	13%	**42%**	**50%**
Human capital	26%	21%	**48%**	22%	12%
Communications/reputation	16%	14%	29%	14%	7%
Market changes/competition	15%	15%	10%	17%	14%
Geopolitical/macroeconomic uncertainty	14%	17%	19%	12%	7%
Health/safety	10%	2%	10%	17%	24%
Climate change/environment	8%	5%	8%	8%	24%
Mergers/acquisitions	5%	2%	8%	5%	7%

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 = 512 for Latin America.

Sector differences

Sector differences show that CAEs must calibrate audit plans to the organization's operating model (Exhibit 2.3).

Cybersecurity and fraud are generally high internal audit priorities across all sectors. In financial services, priority is also high for financial/liquidity, regulatory change, and digital disruption. Privately held and publicly traded organizations share higher priority for supply chain risks, while the public sector has substantially higher priority for governance, organizational culture, and human capital.

The sector analysis reinforces a central message: internal audits should not use regional rankings mechanically. The rankings should be used as a challenge tool. CAEs should compare the regional results to their organization's risk assessment, strategy, stakeholder expectations, operating model, industry dynamics, and existing assurance map. Audit plans should also remain flexible. Geopolitical, digital, cyber, liquidity, regulatory, and market conditions can change faster than the annual planning cycle. CAEs should therefore build formal refresh points into the audit plan and maintain the ability to reallocate effort when the risk profile changes. The CAE's knowledge and experience within the industry are valuable intangible assets. When combined with a robust audit planning methodology, this industry insight helps internal audit focus on the risks most relevant to the organization's objectives. Where sector risk is high, but audit priority is low, the CAE should determine whether the risk is covered through another assurance provider, embedded in other audits, addressed through advisory work, monitored through periodic updates, or insufficiently covered.

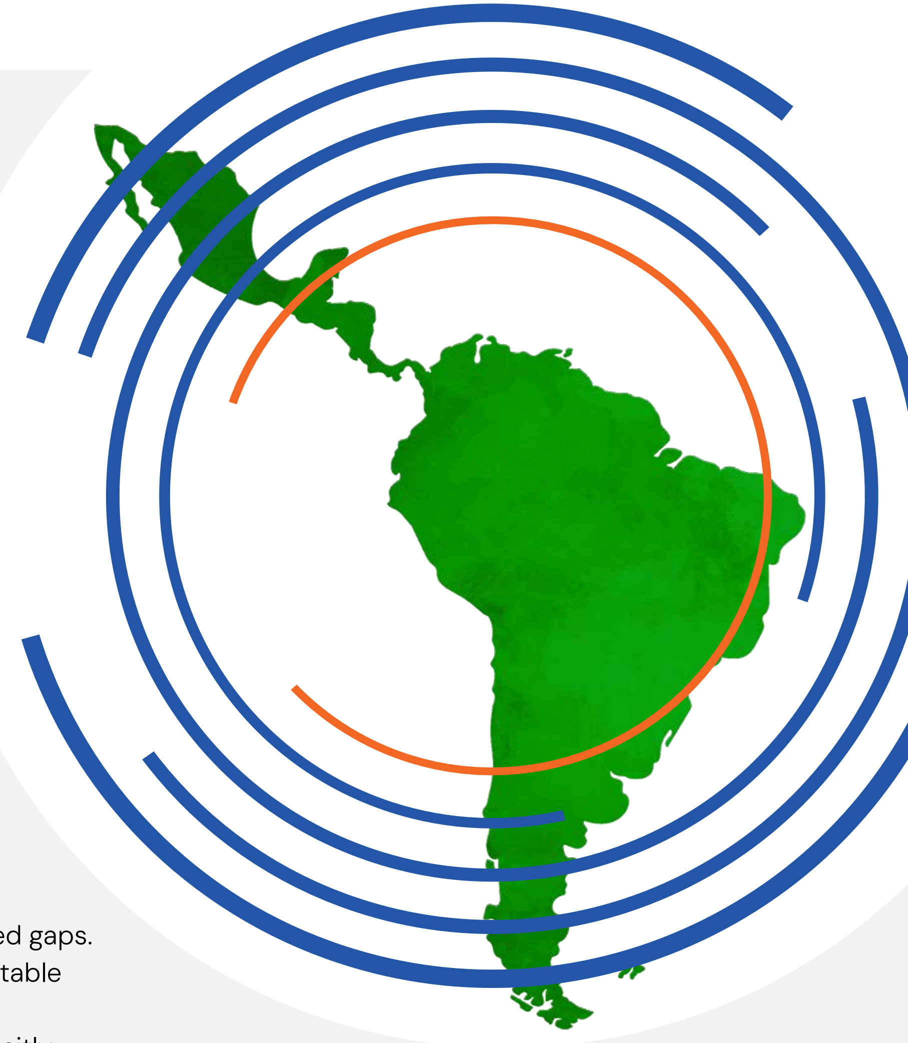
Summary

The implication for CAEs is not that every risk must receive equal coverage. Audit resources are limited. The implication is that the internal audit plan should make the rationale for coverage explicit, keeping organizational strategy in mind, while remaining flexible enough to respond to material changes in the risk environment. Where risk is high, but audit effort is low, the CAE should be able to explain why. Is the risk covered by another assurance provider? Is management's governance mature? Is the risk monitored through advisory work? Is it embedded in other audits? Will the risk be reconsidered during a formal plan refresh? Or is there a true gap due to limited capability or capacity?

> **"Internal audit must move beyond what is comfortable. The question is not only whether we have resources, but whether we are preparing ourselves to audit what the business is becoming."**
>
> **– Ámbar Vargas, Panama**

BACK NEXT CONTENTS

KEY POINTS



Survey insights

- Internal audit effort remains strongest in:
  - Cybersecurity
  - Fraud
  - Financial/liquidity
  - Regulatory change
  - Digital disruption (including AI)

This reflects both risk relevance and the profession's historical strengths.

- The largest gaps are in areas that are harder to audit directly:
  - Geopolitical/macroeconomic uncertainty
  - Market changes/competition
  - Climate change/environment
  - Human capital
  - Organizational culture
  - Some aspects of digital disruption

Internal audit strategies

- CAEs should map all Top 5 risks against current audit coverage and identify unexplained gaps.
- Where risks are difficult to audit directly, internal audit should translate them into auditable processes, decisions, scenarios, and controls.
- Audit plans should include a balance of assurance and advisory work, and should explicitly document how high risks are covered, whether through direct audits, embedded scope, continuous monitoring, reliance on second-line functions, or board-level reporting.

3. RISK MATURITY AND COVERAGE

The Highest Risks Are Not Always the Most Mature or Best Covered

The new governance maturity and internal audit coverage data provide one of the most important insights in this year's report.

Risk level alone does not show whether an organization is ready to manage the risk. Audit priority alone does not show whether internal audit coverage is sufficient. By comparing risk level, governance maturity, and audit coverage, CAEs can identify where the organization may be most exposed.

Risk governance maturity

The survey asked respondents to rate the maturity of risk governance for each risk area. Exhibit 3.1 shows that financial/liquidity has the highest level of mature governance, with 59% rating it as managed or optimized. Regulatory change follows at 47%, governance/corporate reporting at 44%, communications/reputation at 41%, and fraud at 40%. These are areas where organizations often have established frameworks, clear ownership, regulatory expectations, policies, and recurring oversight.

By contrast, digital disruption has the lowest level of mature governance. Only 19% rated governance for digital disruption as managed or optimized, while 57% rated it as initial or infrastructure. Climate change/environment also shows low maturity, with 20% managed or optimized and 56% initial or infrastructure. Geopolitical/macroeconomic uncertainty, human capital, culture, and supply chain also show relatively modest maturity levels.

This pattern is understandable, but risky. Mature governance tends to exist where organizations have had many years to develop processes and where regulatory or financial consequences are clear. Emerging risks often evolve faster than governance. AI, for example, may be adopted by business units before the organization has defined policies, model approval processes, data ownership, monitoring requirements, or escalation protocols. Geopolitical risk may be discussed at the board level, but not translated into risk indicators, scenarios, or operational response plans.

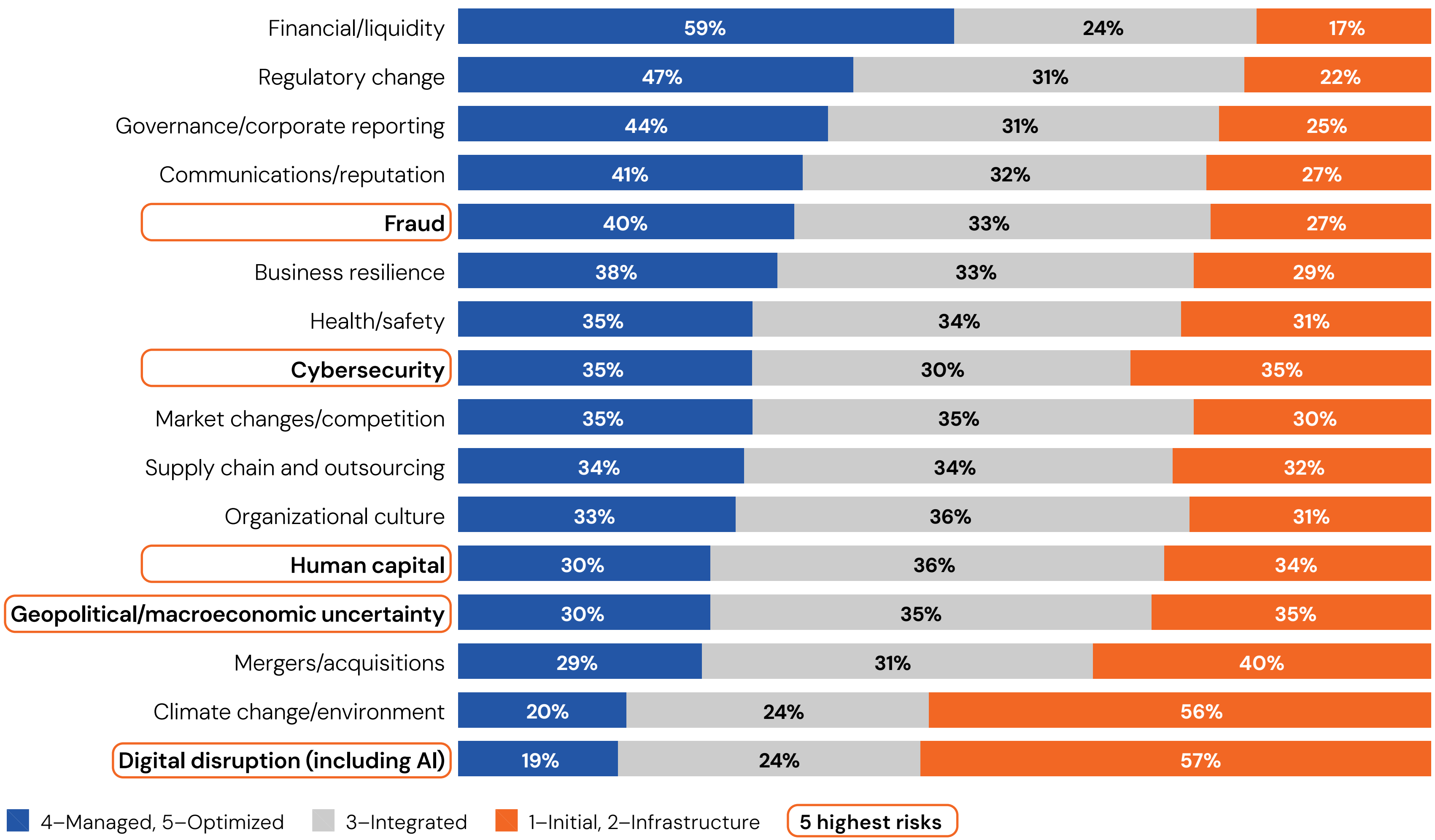
The IIA's guidance on assessing risk management processes reinforces the importance of maturity. Risk management maturity is not only about having policies; it is about whether risk identification, assessment, response, monitoring, communication, and accountability are embedded into decision-making. A low-maturity environment requires a different internal audit approach. In highly mature areas, internal audit can test design and operating effectiveness. In low-maturity areas, internal audit may first need to assess governance design, roles and responsibilities, risk appetite, data availability, escalation, and monitoring.

AI

Digital disruption has the lowest level of risk governance maturity, with only **19%** of Latin American CAEs rating it as managed or optimized.

Exhibit 3.1. Latin America – Risk Governance Maturity

Survey question: **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.**



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

RISK MATURITY AND COVERAGE

Internal audit coverage

Exhibit 3.2 shows a similar concern for internal audit coverage. Financial/liquidity has the highest level of full coverage at 45%, followed by regulatory change at 39%, governance/corporate reporting at 37%, fraud at 30%, and cybersecurity at 26%. These are familiar and necessary areas of coverage.

However, full coverage is lowest for digital disruption at only 8%. Geopolitical/macroeconomic uncertainty is also low at 11%, climate change/environment at 13%, market changes/competition at 14%, organizational culture at 20%, human capital at 20%, and supply chain at 21%. The percentage rating coverage as insufficient is highest for digital disruption at 45%, climate/environment at 37%, geopolitical/macroeconomic uncertainty at 35%, and market changes/competition at 29%.

This creates a clear risk message: some of the areas with the highest strategic relevance have the lowest governance maturity and weakest internal audit coverage. Digital disruption is the most visible example. It is the second-highest Top 5 risk and is rated high by 75%, yet it has the lowest mature governance and lowest full audit coverage. For boards, this should be a red flag. For CAEs, it should be a planning priority.

Rethinking coverage

The solution is not necessarily to add large numbers of new audits. Many internal audit functions in Latin America operate with limited staff and budget. The solution is to rethink coverage. For digital disruption, internal audit can perform advisory reviews of AI governance, data governance, cloud risk, automation controls, third-party technology risk, cybersecurity-by-design, and change management. It can also embed digital risk questions into audits of sales, finance, operations, procurement, HR, and compliance.

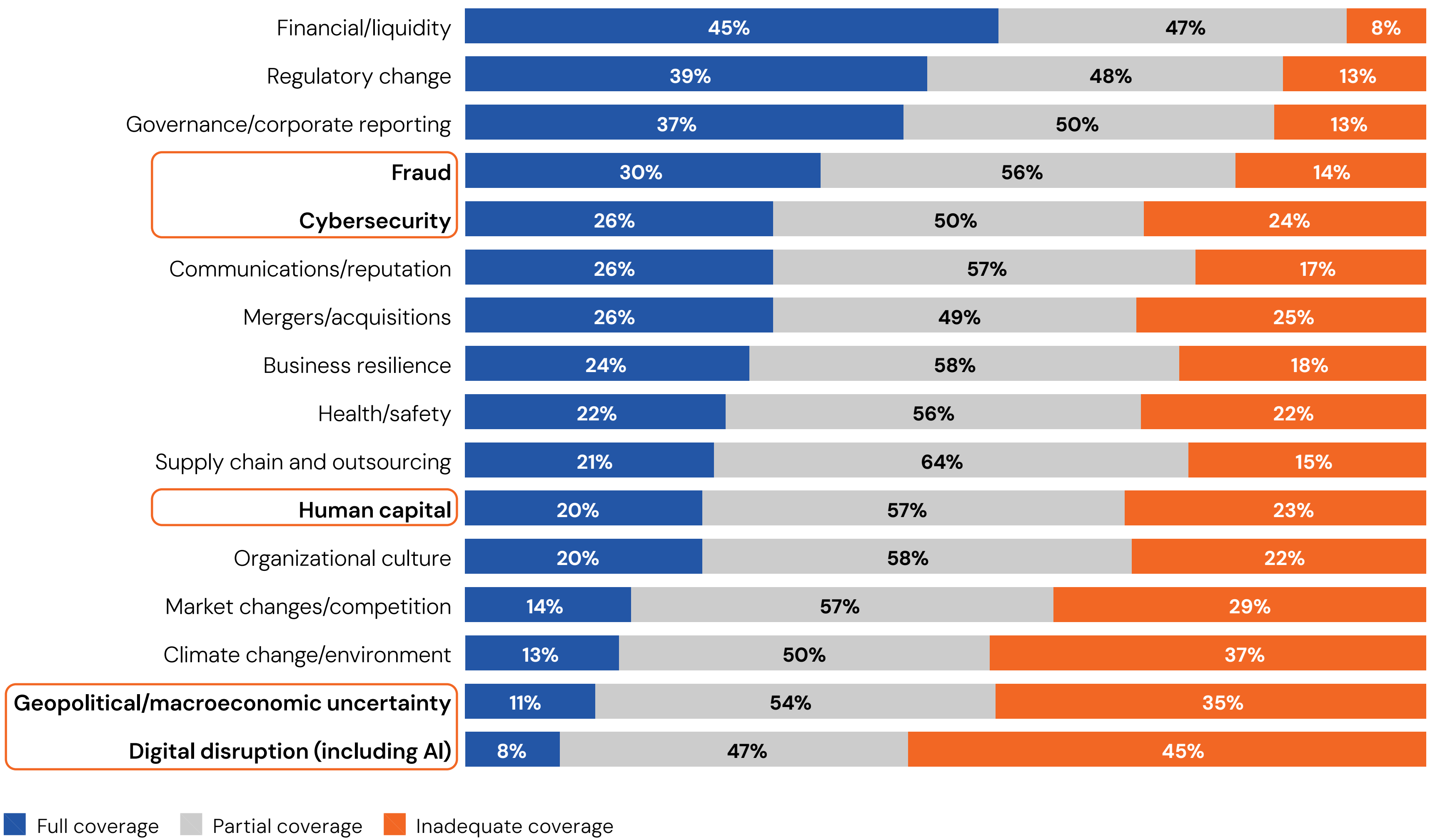
For geopolitical/macroeconomic uncertainty, internal audit can review scenario planning, stress testing, business continuity, crisis management, treasury, supply chain, strategic planning, and regulatory monitoring. For climate/environment, internal audit can focus on physical risk exposure, environmental compliance, sustainability reporting controls, asset resilience, insurance, and continuity planning. For human capital, internal audit can assess strategic workforce planning, critical roles, succession, training, retention, culture, incentives, and capability gaps.

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

– Ámbar Vargas, Panama

Exhibit 3.2. Latin America – Internal Audit Coverage

Survey question: 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* = 512 for Latin America.

RISK MATURITY AND COVERAGE

Coordinating with the second line

The maturity and coverage data also highlight the importance of coordination with the second line. Internal audit does not need to own every risk management activity. However, the CAE should understand who owns the risk, how it is monitored, what assurance exists, and whether the board receives reliable information. In low-maturity areas, advisory work may be more valuable than traditional assurance in the short term, provided objectivity is safeguarded.

Advisory services

Several roundtable participants raised the question of independence when internal audit provides advisory support in emerging areas. This concern is valid, but it should not become an excuse for inaction. The Global Internal Audit Standards™ allow internal audit to provide advisory services, provided the CAE manages potential impairments to objectivity and avoids taking management responsibility. In practice, internal audit can help management understand leading practices, ask better questions, evaluate readiness, and identify gaps without designing or owning controls.

This is especially important for AI and digital transformation. Waiting until controls are fully implemented may be too late. Internal audit can add value earlier by reviewing governance design, decision criteria, risk assessments, vendor due diligence, test approvals, data protection, and monitoring plans. Early involvement does not mean management responsibility. It means timely assurance and advice in an area where risk is moving quickly.

Summary

For CAEs, maturity and coverage analysis should become part of the annual audit planning conversation with the board. The CAE should present not only the highest risks, but also the areas where governance is immature and coverage is insufficient. This allows the board to see where risk may be accumulating silently.

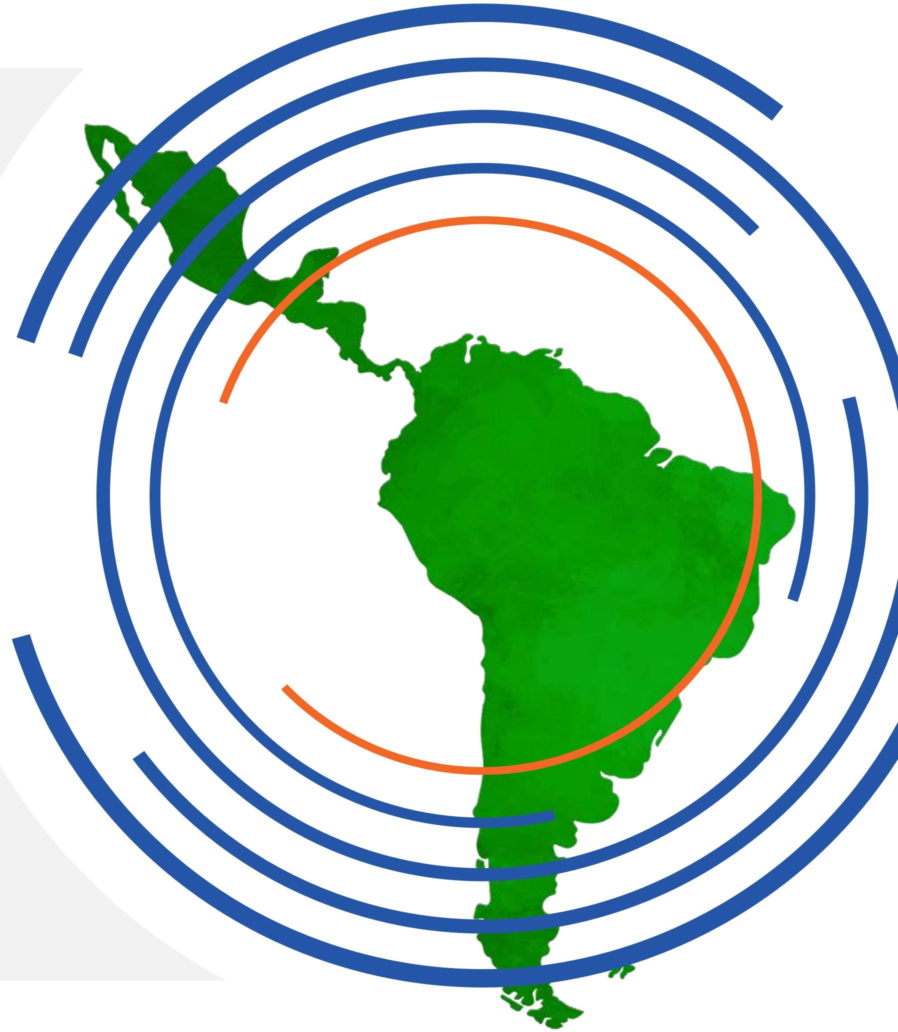
KEY POINTS

Survey insights

- The highest governance maturity and strongest audit coverage are concentrated in more traditional areas such as financial/liquidity, regulatory change, governance/corporate reporting, fraud, and cybersecurity.
- The weakest maturity and coverage are in emerging or strategic areas such as digital disruption, geopolitical/macroeconomic uncertainty, climate/environment, market changes, culture, and human capital.
- Digital disruption stands out as the most urgent gap because it is both a high risk and an area of low maturity and low coverage.

Internal audit strategies

- CAEs should create a "risk-maturity-coverage" view for the board. High-risk areas with low maturity and low audit coverage should be discussed explicitly. Internal audit should use advisory engagements, readiness assessments, embedded audit procedures, and coordinated assurance to address emerging risks before they become control failures.
- Audit plans should identify not only what will be audited, but also why certain high-risk areas receive limited coverage and how that gap will be monitored.



CONCLUSION

The CAE as Translator of Risk, Strategy, and Action

Latin America's 2026/2027 Risk in Focus results show that the region is entering a demanding phase of risk management and internal audit leadership.

The main risks are visible. Cybersecurity, digital disruption, geopolitical/macroeconomic uncertainty, fraud, human capital, regulation, and liquidity are already on the radar of CAEs, executives, and boards. The challenge is no longer only awareness. The challenge is action.

For internal audit, this means moving from a risk-ranking mindset to a risk-response mindset. A high risk that does not influence audit planning, assurance coverage, advisory activity, talent strategy, or board dialogue remains only a survey result. The value of Risk in Focus is realized when CAEs use it to challenge their audit universe, test assumptions, and ask whether the function is focusing on the risks that matter most to organizational value. The findings point to three priorities for CAEs in Latin America:

1. Internal audit must address connected risks. Cybersecurity, AI, fraud, data, regulation, third parties, liquidity, reputation, and continuity should not be audited only as separate silos. The most damaging events often occur at the intersection of risks. A cyber incident can become a fraud event, a regulatory breach, a liquidity issue, and a reputational crisis. A geopolitical event can become a supply chain issue, a cloud resilience issue, a foreign exchange issue, and a business continuity issue.
2. CAEs must close the gap between emerging risks and audit capability. Digital disruption has become one of the highest risks in the region, but governance maturity and audit coverage remain low. This gap cannot be solved only by hiring specialists, although specialized skills are important. It also requires new methodologies, training, co-sourcing, data analytics, continuous auditing, stronger coordination with the second line, and more strategic conversations with management.
3. Internal audit must strengthen its relationship with the board and executive management. The CAE should be close enough to strategy to understand where the organization is going, while maintaining objectivity to assess whether risks are being managed appropriately. This balance is not a weakness in independence; it is a requirement for relevance.

The next generation of internal audit leadership in Latin America will be defined by the ability to translate volatility into decisions. Boards need CAEs who can explain how global trends affect local operations, how emerging technologies change control environments, how talent gaps affect strategic execution, and how audit coverage must evolve.

The most important question for 2027 is not whether internal audit understands the risk landscape. It is whether internal audit is prepared to act on it.

> **"Internal audit cannot point in the right direction if it does not understand where the organization is going."**
>
> **– Héctor Trujeque, Argentina**

BACK NEXT CONTENTS

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.

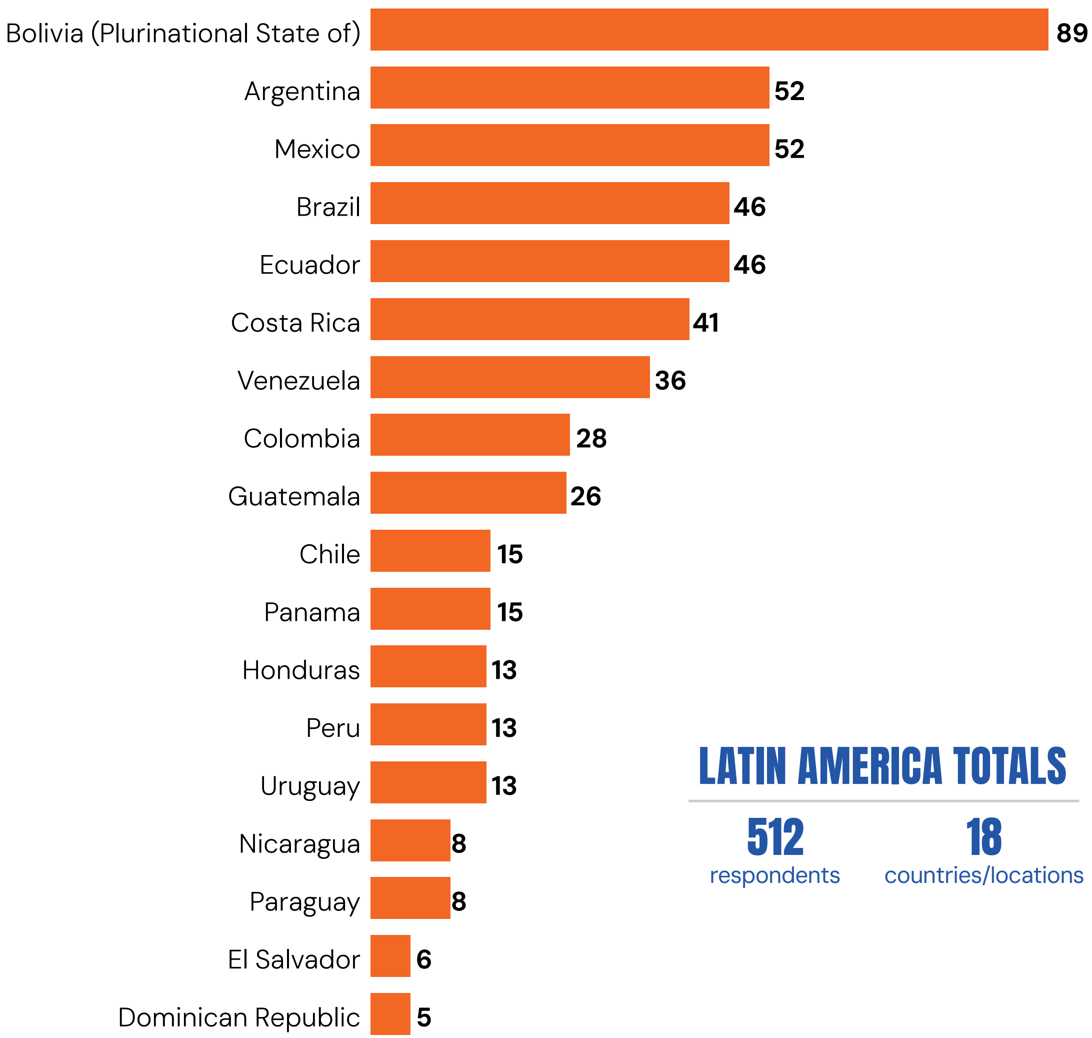
Completed surveys were received from 3,285 internal auditors who confirmed that they were the highest-ranking internal auditor at their organizations. They represented 132 countries/locations. The survey was conducted online through contacts associated with IIA National Institutes and regional bodies. 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 'n^{th}' party risk

APPENDIX B. DEMOGRAPHICS

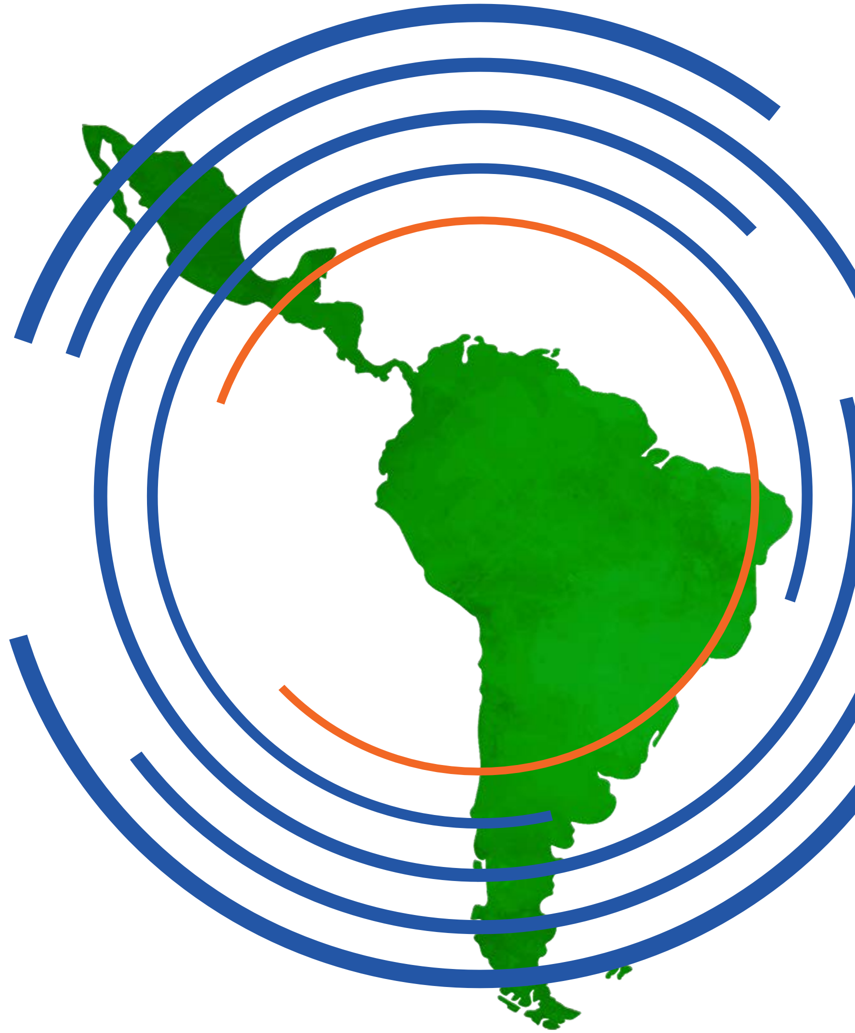
Exhibit B.1. Latin America – Response Rate



LATIN AMERICA TOTALS

512 respondents

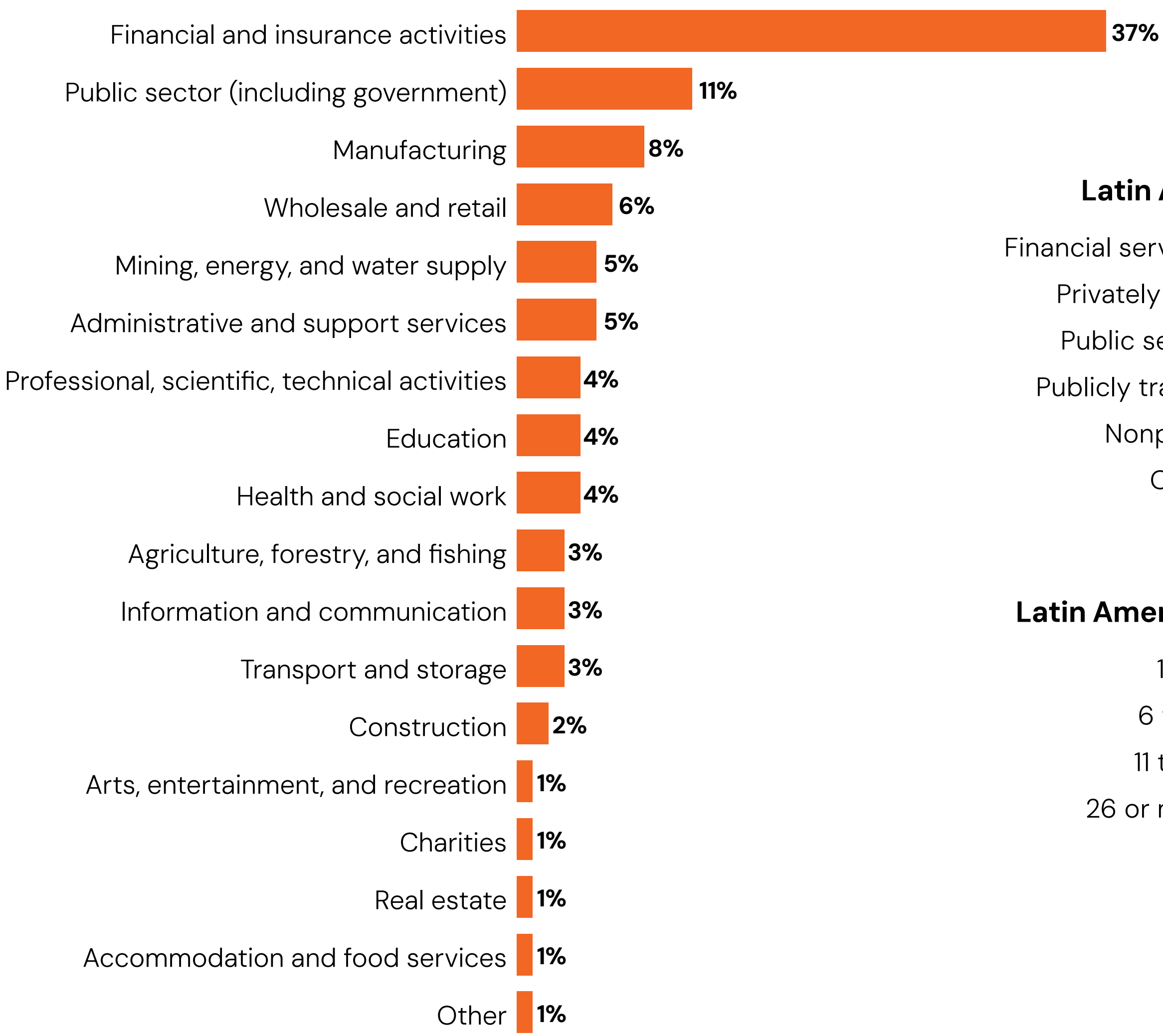
18 countries/locations



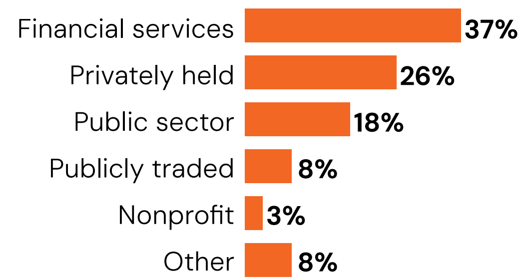
Note: Risk in Focus survey conducted online worldwide from March 2 to May 6, 2026. *n* = 512 for Latin America.

Exhibit B.2. Latin America – Industry, Organization Type, Internal Audit Size

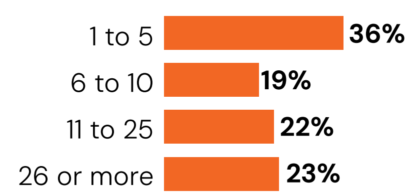
Latin America – Industry



Latin America – Organization Type



Latin America – Internal Audit Function Size



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

APPENDIX C. GLOBAL RISK OVERVIEW

Latin America in a Global Pattern of Acceleration

Latin America's risk environment is part of a broader global trend. The global pattern matters for CAEs in Latin America because many organizations in the region operate across borders, depend on global technology providers, import critical supplies, use international financial markets, and are affected by global cyber threat actors. Even organizations that operate locally are exposed to global risk transmission through inflation, foreign exchange, cloud platforms, software providers, cybercrime networks, regulation, and consumer behavior.

Survey results show that regions around the world are experiencing similar risk trends (Exhibit C.1 and Exhibit C.2):

- Risk ratings for digital disruption increased in every region of the world.
- Cybersecurity and geopolitical uncertainty increased for all but one region, North America.
- Fraud and financial/liquidity risks increased for Africa, Asia Pacific, and Latin America.
- Supply chain risk increased for Africa, Asia Pacific, and the Middle East.

Gaining perspective from global context

The global context should not lead CAEs to copy global priorities without adaptation. Rather, it should help them challenge local assumptions. A global trend may not be a high risk for every organization, but it should be considered in the risk assessment. For example, climate/environment may rank lower for Latin America overall than cybersecurity or AI, but for energy, agriculture, infrastructure, transport, mining, insurance, and government, it may be a strategic risk. Similarly, supply chain risk may not be high for an airline's onboard food supply, but it may be critical for healthcare, retail, manufacturing, or energy.

For boards and audit committees, the value of global comparison is benchmarking. It helps answer three questions: Are we seeing the same risks as peers? Are we moving faster or slower than the market? Are there risks rising globally that we have not yet translated into our strategy? CAEs should use global comparisons not as a substitute for enterprise risk assessment, but as a challenge mechanism to improve it.

Internal audit can also use global comparison to support resource discussions. If digital disruption, cybersecurity, and geopolitical uncertainty are rising worldwide, but the internal audit function lacks technology skills, data analytics, cyber expertise, or strategic risk capability, the CAE has a stronger case for investment. The conversation with the board should move from "we need more resources" to "our risk profile has changed, and our capabilities must change with it."

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

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

Graphic designers
Sergio Analco and
Cathy Watanabe

INTERNAL AUDIT FOUNDATION PARTNERS

DIAMOND PARTNERS

GOLD PARTNERS

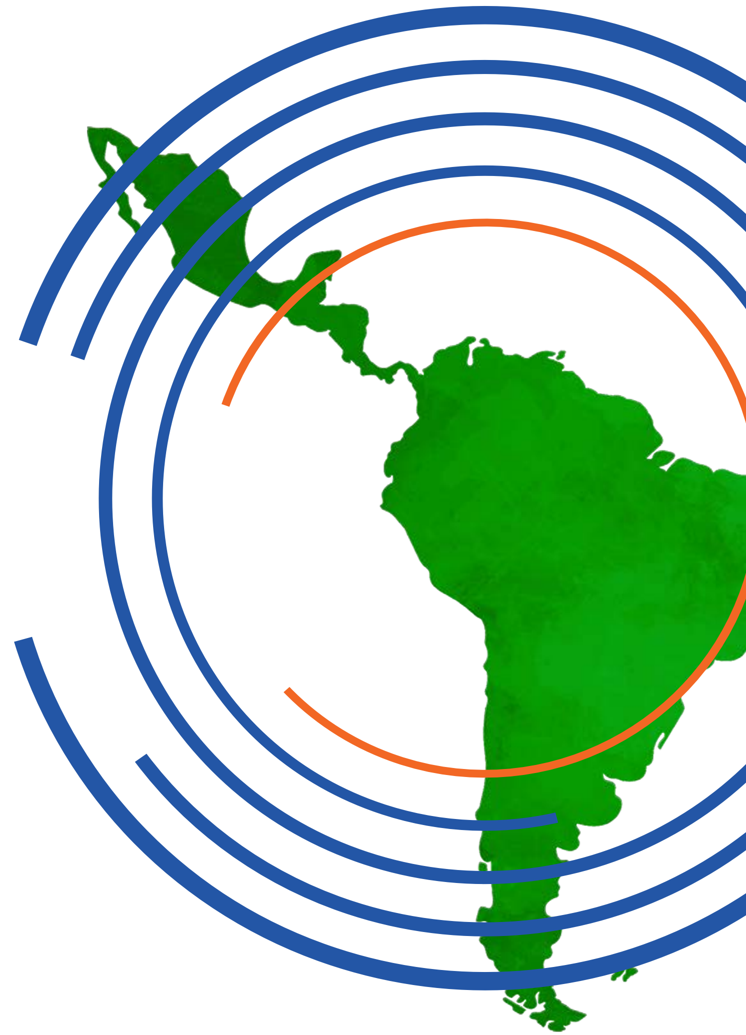
- Carr, Riggs & Ingram
- Fundación Latinoamericana de Auditores Internos
- IIA–Houston Chapter
- IIA–Japan
- IIA–New York Chapter
- IIA–San Francisco Chapter

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

FUNDACION LATINOAMERICANA DE AUDITORES INTERNOS (FLAI)



FLAI Board

President
Geraldine Giachello, CIA, CPA
Vice President
Manuel Quezada, CPA, MBA
Secretary and Past President
Francisco Arauz, CIA, CCSA, CPA
Treasurer
Maritza Barzola, CRMA, CPCC
Board Members
Javier Ferrer, CPA, Master in Executive Management
Marcia Pereira, CIA, CCSA
Jim Romero, CIA, CCSA, CRMA, CPA

FLAI Executive Director

Roberto Loo

Writer

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

Risk in Focus Roundtable Moderators

Savio Jannuzzi, Brazil
Alejandro Rembado, Argentina

THANK YOU!

The research development team thanks the internal audit leaders across Latin America who participated in the survey, roundtables, and interviews. Their practical insights helped transform survey results into a more actionable understanding of how risks are evolving in the region and how internal audit functions can respond with greater relevance, agility, and strategic impact.

Fundación Latinoamericana
de Auditores Internos

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
The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

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