2024 RISK IN FOCUS

Hot topics for internal auditors

LATIN AMERICA

Read more

Internal Audit FOUNDATION

FLAI
Fundación Latinoamericana de **Auditores Internos**

ABOUT RISK IN FOCUS

Risk in Focus provides practical, data-driven research to help internal auditors and their stakeholders understand today's risk environment and prepare audit plans for the year ahead.

Reports are based on a worldwide survey to identify current and emerging risks for each region, followed up with roundtables and interviews to discover leading practices for internal auditors.

Two reports are created for each region:

- **Hot Topics for Internal Auditors** – Detailed reports based on the survey, roundtables, and interviews.
- **Board Briefing** – Summary reports for internal auditors to share with stakeholders.

Global Risk in Focus is a collaborative partnership facilitated by the Internal Audit Foundation with generous support from IIA regional bodies, IIA Institutes, and corporate sponsors. 2024 marks the first year the project was conducted worldwide.

The Risk in Focus methodology was originally created in 2016 by the European Institutes Research Group (EIRG), which continues to publish it in Europe through the European Confederation of Institutes of Internal Auditing (ECIIA).

Reports are available free to the public at The IIA's Risk in Focus resource page and at the websites for IIA regional groups: ACIIA (Asia Pacific), AFIIA (Africa), ARABCIIA (Middle East), ECIIA (Europe), FLAI (Latin America).

LATIN AMERICA REPORT SPONSORS

FLAI
Fundación Latinoamericana de Auditores Internos

GRUPO BIMBO
ALIMENTAMOS UN MUNDO MEJOR

Translations Sponsor

IIA–Argentina
IIA–Bolivia
IIA–Brazil
IIA–Chile
IIA–Colombia
IIA–Costa Rica
IIA–Dominican Republic
IIA–Ecuador
IIA–El Salvador
IIA–Guatemala
IIA–Honduras
IIA–Mexico
IIA–Nicaragua
IIA–Panama
IIA–Paraguay
IIA–Peru
IIA–Uruguay
IIA–Venezuela

CONTENTS

Contents

EXECUTIVE SUMMARY – LATIN AMERICA
Building relationships to succeed together

Rolling elections and political uncertainty have complicated the emerging risk landscape in Latin America as organizations attempt to rebound from the pandemic. Countries in the region are striving to establish closer relationships to build back their economies and create or unify rules in areas such as anti-money-laundering and cybersecurity.

Latin America Risk in Focus 2024 provides insight into essential questions for organizations and their boards, including:

- What are the top risks organizations face in the region? How will these develop over the next three years?
- Where are internal auditors investing the most time and effort?
- How can internal audit functions help their organizations?

Cybersecurity, regulatory change, and business continuity were the three highest risk areas cited by CAEs in Latin America for 2024 (see Figure 5). CAEs also allocated the most internal audit effort to the first two categories (see Figure 7). Climate change and digital disruption are expected to be the biggest climbing risks for organizations in Latin America in the next three years, and both are expected to see steep rises in internal audit effort (see Figures 6 and 8).

Among survey respondents worldwide, the three areas of highest risk were cybersecurity, human capital, and business continuity (see Figure 1). Across regions there was remarkable consensus that digital disruption and climate change were the two areas expected to increase the most for risk level and audit effort (see Figure 3).

The Latin America Risk in Focus reports describe in detail the challenges and solutions for urgent risk areas and draw on

Latin America Research Participation

- **956 survey responses** from CAEs and directors
- **25 participating countries/territories**
- **2 roundtables** with 18 participants
- **5 in-depth interviews**

Contents

EXECUTIVE SUMMARY – LATIN AMERICA

the expertise, experience, and knowledge of multiple internal audit leaders throughout the region. The featured topics for the Latin American reports are:

Cybersecurity – Where local cybersecurity frameworks are lacking, CAEs draw on international standards to boost the cyber maturity of their organizations.

Business continuity – Continuity plans are being used not only to deal with emerging risks, but also to identify new opportunities and solve unexpected problems.

Geopolitical uncertainty – Scenario role-playing has helped boards plan strategic responses to potentially large-scale, rapid political change.

For a summary of findings to provide to boards and stakeholders, see Latin America Risk in Focus 2024 – Board Briefing. For reports from other regions, see the Risk in Focus resource page.

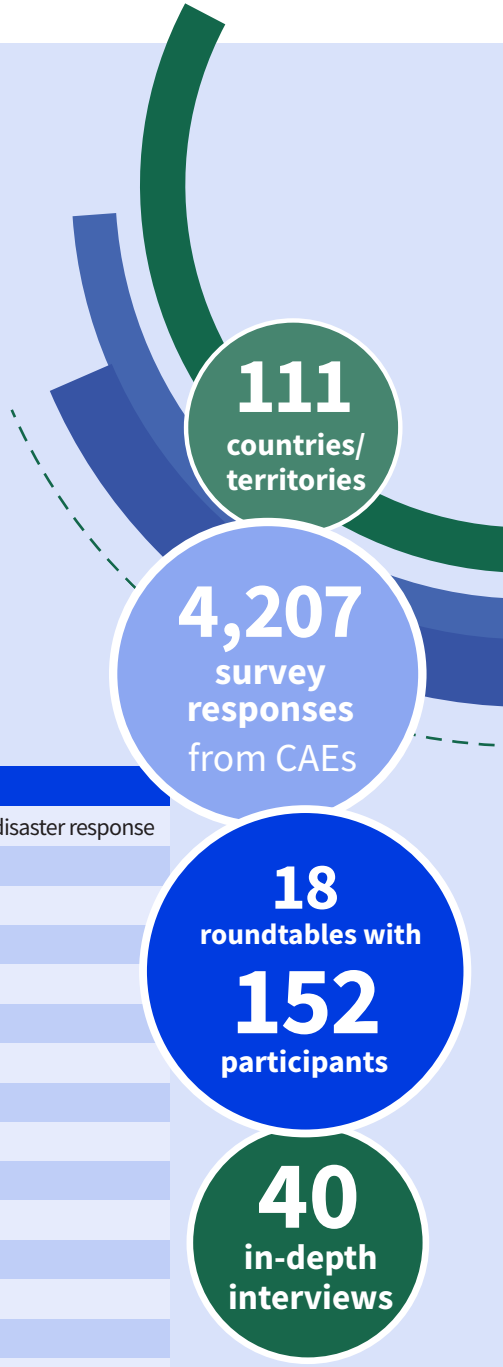
Contents

METHODOLOGY

The Risk in Focus methodology starts with a survey of CAEs and heads of internal audit to identify current and emerging risks for each region. The top risks identified in the survey are used in follow-up roundtables and interviews with CAEs, academics, and other industry experts.

The survey presents 16 risk categories, shown below. Respondents are asked to choose the top 5 highest for risk level and the top 5 highest for internal audit time and effort – both for now and three years in the future. In reports, the categories are referenced by their shortened names.

For the Risk in Focus 2024 project worldwide, survey responses were received from 4,207 CAEs and directors in 111 countries/territories from February 15 to July 12, 2023. Eighteen roundtables were conducted with 152 participants, followed by 40 in-depth interviews.



Risk in Focus 2024 Risk Categories

Risk Topic	Risk Description Used in the Survey
Business continuity	Business continuity, operational resilience, crisis management, and disaster response
Climate change	Climate change, biodiversity, and environmental sustainability
Communications/reputation	Communications, reputation, and stakeholder relationships
Cybersecurity	Cybersecurity and data security
Digital disruption	Digital disruption, new technology, and AI
Financial liquidity	Financial, liquidity, and insolvency risks
Fraud	Fraud, bribery, and the criminal exploitation of disruption
Geopolitical uncertainty	Macroeconomic and geopolitical uncertainty
Governance/corporate reporting	Organizational governance and corporate reporting
Health and safety	Health, safety, and security
Human capital	Human capital, diversity, and talent management and retention
Market changes	Market changes/competition and customer behavior
Mergers and 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

SURVEY RESULTS – GLOBAL

Regional comparisons

The worldwide participation in the Risk in Focus survey provides a rare opportunity to compare risk and audit planning between different regions.

How to use survey results

The Risk in Focus survey results are presented in a series of graphs that show survey responses about risk levels and audit effort – both now and three years in the future. Key findings from responses worldwide are summarized as follows, but readers are encouraged to review the graphs in detail to obtain further insights.

Percentages show how many chose an audit area as one of the five highest for risk level or audit effort at their organization.

In the graphs, results for risk levels are colored blue, and results for audit effort are green; current levels are darker shades and future levels are lighter.

Figure 1: Top 5 highest risks per region – Global

There is broad consensus worldwide that the three areas of highest risk for the organizations where CAEs work are:

1. Cybersecurity
2. Human capital
3. Business continuity

For most regions, regulatory change also ranks as a top 5 highest risk, with the exception of Africa and Middle East, where financial liquidity is more of a concern. Reflecting current events and future concerns, geopolitical instability rounded out the list for Latin America and Europe. Market changes were considered a top risk for Asia Pacific and North America, but not in other regions.

Global Survey – Responses Per Region

Africa	808
Asia Pacific	1,035
Latin America (& Caribbean)	956
Europe	799
North America	442
Middle East	167
Total	**4,207**

SURVEY RESULTS – GLOBAL

Finally, Africa was the only region with fraud as a top 5 concern, while the Middle East was unique for having governance/corporate reporting in their top 5.

Another way to look at the data is to consider which region had the highest risk within each audit area. For example, climate change risks were rated highest in Europe, compared to other regions. Some notable points about highest ratings per audit area include:

- North American respondents gave cybersecurity (85%) and human capital (65%) the highest risk ratings compare to other regions.
- For Europe, while cybersecurity was nearly as high as for North America (84%), the other areas of high concern were geopolitical uncertainty (43%) and climate change (31%). Europe was the only region where climate change was higher than 30%.
- Latin America shared Europe's concern about geopolitical uncertainty (42%), but also reported high risk for regulatory change (48%) and digital disruption (38%).
- Asia Pacific was particularly concerned with business continuity (61%) and market changes (47%), compared to other regions.
- The Middle East had much higher risk levels for governance/corporate reporting (45%) than other regions and was also slightly higher for communications/reputation (28%).
- Finally, Africa had a unique mix of risks that were higher than other regions, including financial liquidity (47%), fraud (46%), and organizational culture (34%).

Figure 2: Top 5 audit effort per region – Global

Although risk levels may vary from region to region, the areas of highest effort for internal audit are remarkably similar, generally in this order:

1. Cybersecurity
2. Governance/corporate reporting
3. Business continuity
4. Regulatory change
5. Financial liquidity
6. Fraud

Although risk levels may vary from region to region, the areas of highest effort for internal audit are remarkably similar.

The primary area of difference was for regulatory change, where audit effort percentages were notably lower for Africa (35%) and Middle East (35%) than other regions, which were at 50% or higher.

Other specific differences were:

- Asia Pacific had a lower percentage for financial liquidity (35%) than the global average (45%).
- Latin America was lower than other regions for effort toward governance/corporate reporting (46% for Latin America vs. 55% global average).
- North America was much lower than the global average for fraud effort (26% for North America vs. 42% global average).

SURVEY RESULTS – GLOBAL

An additional way to look at the data is to consider which region had the highest audit effort within each audit area. In many audit areas, the difference in effort between regions is small. But there were some audit areas where differences were notable:

- North America was much more broadly involved in cybersecurity (84%) than other regions, with the exception of Europe (79%).
- Africa has more functions putting top 5 effort toward fraud (57%) and financial liquidity (53%) than other regions.
- Europe has almost double the percentage who say climate change is top 5 for audit effort (19%) compared to the global average (11%).

Figure 3: Expected risk change in three years – Global

There is consensus worldwide that risk levels will rise in the next three years for digital disruption and climate change. Both areas saw increases of about 20 percentage points between current and future risk levels. Even more remarkable is the increase in ranking for climate change, which leaped from fourteenth place to fifth.

Figure 4: Expected audit effort change in three years – Global

With risk levels expected to rise for digital disruption and climate change, so is the amount of time and effort internal audit expects to spend in these areas. The percentage expecting digital disruption to be top 5 for audit effort more than doubled - from 22% to 52%. Equally remarkable, the percentage for climate change more than tripled, from 11% to 34%.

There is consensus worldwide that risk levels will rise in the next three years for digital disruption and climate change.

Figure 1:

Top 5 highest risks per region – Global

Highest risks per region

There is broad consensus worldwide that the three areas of highest risk are cybersecurity, human capital, and business continuity.

What are the top 5 risks your organization currently faces?

Audit area	Average of all regions	Asia Pacific	Latin America	Africa	North America	Middle East	Europe
Cybersecurity	**73%**	**66%**	**75%**	**58%**	**85%**	**70%**	**84%**
Human capital	**51%**	**59%**	**44%**	**39%**	**65%**	**47%**	**50%**
Business continuity	**47%**	**61%**	**47%**	**52%**	**36%**	**53%**	**35%**
Regulatory change	**39%**	**35%**	**48%**	32%	**43%**	33%	**43%**
Digital disruption	**34%**	30%	38%	33%	36%	32%	33%
Financial liquidity	**32%**	21%	33%	**47%**	28%	**38%**	26%
Market changes	**32%**	**47%**	26%	21%	**41%**	26%	30%
Geopolitical uncertainty	**30%**	28%	**42%**	25%	28%	16%	**43%**
Governance/corporate reporting	**27%**	24%	18%	36%	16%	**45%**	22%
Supply chain and outsourcing	**26%**	27%	16%	19%	36%	28%	30%
Organizational culture	**26%**	23%	26%	34%	21%	30%	20%
Fraud	**24%**	22%	30%	**46%**	9%	26%	13%
Communications/reputation	**21%**	18%	22%	27%	21%	28%	12%
Climate change	**19%**	22%	22%	19%	12%	10%	31%
Health and safety	**11%**	12%	8%	10%	17%	9%	13%
Mergers and acquisitions	**6%**	4%	3%	3%	8%	10%	8%

Note: The IIA's Risk in Focus Global Survey, *n* = 4,207. Percentages show who ranked the area as one of their top 5 for risk level. Dark blue shading indicates the 5 areas of highest risk for that region.

Figure 2:

Top 5 audit effort per region – Global

Highest effort areas per region

■ The areas of highest audit effort across regions are remarkably similar.

What are the top 5 risks on which internal audit spends the most time and effort?

Audit area	Average of all regions	Asia Pacific	Latin America	Africa	North America	Middle East	Europe
Cybersecurity	**68%**	**66%**	**66%**	**54%**	**84%**	**61%**	**79%**
Governance/corporate reporting	**55%**	**54%**	46%	**52%**	**55%**	**64%**	**61%**
Business continuity	**54%**	**59%**	**53%**	**56%**	**53%**	**53%**	**50%**
Regulatory change	**46%**	**56%**	**50%**	35%	**53%**	35%	**50%**
Financial liquidity	**45%**	35%	**50%**	**53%**	**46%**	**44%**	**45%**
Fraud	**42%**	**42%**	**47%**	**57%**	26%	**43%**	36%
Supply chain and outsourcing	**34%**	33%	28%	32%	38%	39%	36%
Human capital	**30%**	33%	28%	33%	26%	35%	26%
Organizational culture	**24%**	23%	29%	27%	17%	27%	21%
Digital disruption	**22%**	19%	24%	24%	25%	20%	21%
Communications/reputation	**20%**	21%	23%	25%	20%	23%	11%
Health and safety	**17%**	18%	12%	13%	21%	16%	19%
Market changes	**16%**	23%	17%	15%	14%	16%	10%
Climate change	**11%**	10%	8%	11%	9%	7%	19%
Geopolitical uncertainty	**9%**	6%	13%	12%	4%	8%	8%
Mergers and acquisitions	**6%**	3%	5%	2%	10%	8%	9%

Note: The IIA's Risk in Focus Global Survey, *n* = 4,207. Percentages show who ranked the area as one of their top 5 for audit time and effort. Dark green shading indicates the 5 highest audit effort areas for that region.

Figure 3:

Expected risk change in 3 years – Global

Expected risk change

- Climate change risks are expected to increase dramatically to fifth place up from fourteenth place.
- Digital disruption is expected to increase from 34% to 55% who see it as a top 5 risk.

What are the top 5 risks your organization currently faces?

1.	Cybersecurity	73%
2.	Human capital	51%
3.	Business continuity	47%
4.	Regulatory change	39%
5.	**Digital disruption**	**34%**
6.	Financial liquidity	32%
7.	Market changes	32%
8.	Geopolitical uncertainty	30%
9.	Governance/corporate reporting	27%
10.	Supply chain and outsourcing	26%
11.	Organizational culture	26%
12.	Fraud	24%
13.	Communications/reputation	21%
14.	**Climate change**	**19%**
15.	Health and safety	11%
16.	Mergers and acquisitions	6%

What are the top 5 risks your organization will face 3 years from now?

1.	Cybersecurity	67%
2.	**Digital disruption**	**55%**
3.	Human capital	46%
4.	Business continuity	41%
5.	**Climate change**	**39%**
6.	Regulatory change	39%
7.	Geopolitical uncertainty	34%
8.	Market changes	33%
9.	Supply chain and outsourcing	25%
10.	Financial liquidity	23%
11.	Organizational culture	21%
12.	Governance/corporate reporting	20%
13.	Fraud	20%
14.	Communications/reputation	15%
15.	Health and safety	11%
16.	Mergers and acquisitions	11%

Note: The IIA's Risk in Focus Global Survey, *n* = 4,207. Percentage who ranked the area as one of their organization's top 5 highest risks.

Figure 4:

Expected audit effort change in 3 years – Global

Expected effort change

Steep rises are expected for internal audit activity related to digital disruption and climate change.

What are the top 5 risks on which internal audit spends the most time and effort?

1.	Cybersecurity	68%
2.	Governance/corporate reporting	55%
3.	Business continuity	54%
4.	Regulatory change	46%
5.	Financial liquidity	45%
6.	Fraud	42%
7.	Supply chain and outsourcing	34%
8.	Human capital	30%
9.	Organizational culture	24%
10.	**Digital disruption**	**22%**
11.	Communications/reputation	20%
12.	Health and safety	17%
13.	Market changes	16%
14.	**Climate change**	**11%**
15.	Geopolitical uncertainty	9%
16.	Mergers and acquisitions	6%

What are the top 5 risks you expect internal audit to spend the most time and effort addressing 3 years from now?

1.	Cybersecurity	73%
2.	**Digital disruption**	**52%**
3.	Business continuity	49%
4.	Regulatory change	37%
5.	Governance/corporate reporting	36%
6.	Human capital	35%
7.	**Climate change**	**34%**
8.	Fraud	29%
9.	Financial liquidity	28%
10.	Supply chain and outsourcing	28%
11.	Organizational culture	24%
12.	Market changes	22%
13.	Communications/reputation	16%
14.	Geopolitical uncertainty	16%
15.	Health and safety	15%
16.	Mergers and acquisitions	8%

Note: The IIA's Risk in Focus Global Survey, *n* = 4,207. Percentage who ranked the area as one of their organization's top 5 highest risks.

SURVEY RESULTS – LATIN AMERICA

How to use survey results

Key findings for Latin America are summarized, but readers are encouraged to review the graphs that follow in detail to obtain further insights.

Percentages show how many chose an audit area as one of the five highest for risk level or audit effort at their organization. Results for risk levels are colored blue, and results for audit effort are green; current levels are darker shades and future levels are lighter.

Figure 5: Current risk levels vs. future risk levels

- Cybersecurity stood out at the top of the risk landscape for Latin America for 2024.
- In the next 3 years, digital disruption and climate change are the risks expected to increase the most.

Figure 6: Expected risk change in three years

- Digital disruption is expected to move to second place, with 56% saying it will be a top 5 risk.
- Climate-related risk leaps into fifth position, with 41% saying it will be a top 5 risk.

Figure 7: Current audit effort vs. future audit effort

- Latin American CAEs were most likely to choose cybersecurity as one of their top 5 areas for internal audit effort (66%).
- A wide variety of areas followed close behind cybersecurity for internal audit effort, including business continuity, financial liquidity, and regulatory change.

Latin America & Caribbean Survey Responses Per Country

Mexico	140	Dominican Republic	27
Colombia	121	Uruguay	27
Argentina	78	El Salvador	25
Brazil	69	Paraguay	21
Venezuela	67	Trinidad and Tobago	15
Costa Rica	59	Honduras	13
Nicaragua	54	Barbados	3
Ecuador	52	Jamaica	3
Bolivia	43	Aruba	1
Guatemala	38	Bahamas	1
Chile	35	Cayman Islands	1
Panama	31	Saint Kitts and Nevis	1
Peru	31	**TOTAL**	**956**

Note: For reporting purposes, countries and territories in the Caribbean are included with Latin America.

SURVEY RESULTS – LATIN AMERICA

Figure 8: Expected audit effort change in three years

- Steep rises are expected for activity to deal with digital disruption and climate change.
- Increases are offset by reductions for financial liquidity, regulatory change, and fraud.

Figure 9: Current risk levels vs. current audit effort

- Effort is relatively high compared to risk for governance/corporate reporting, fraud, and financial liquidity.
- Effort is low compared to risk for geopolitical uncertainty, market changes, and climate change, but audit effort to address these may cross over to other areas.

Figure 10: Future risk levels vs. future audit effort

- In 3 years, CAEs expect the gap between key risks and the internal audit effort to narrow in most areas. But the effort will remain relatively low compared to the risk in geopolitical uncertainty and human capital.
- Cybersecurity and digital disruption are expected to share top billing for both risk and audit effort.

Figure 5:

Current risk levels vs. future risk levels – Latin America

- Cybersecurity stood out at the top of the risk landscape for Latin America for 2024.
- In the next 3 years, digital disruption and climate change are the risks expected to increase the most.

What are the top 5 risks your organization currently faces?

What are the top 5 risks your organization will face 3 years from now?

Note: The IIA's Risk in Focus Global Survey, Latin America, *n* = 956. Percentage who ranked the area as one of their organization's top 5 highest risks.

Figure 6:

Expected risk change in 3 years – Latin America

Expected risk change

- Digital disruption is expected to move to second place, with 56% saying it will be a top 5 risk.
- Climate-related risk leaps into fifth position, with 41% saying it will be a top 5 risk.

What are the top 5 risks your organization currently faces?

1.	Cybersecurity	75%
2.	Regulatory change	48%
3.	Business continuity	47%
4.	Human capital	44%
5.	Geopolitical uncertainty	42%
6.	**Digital disruption**	**38%**
7.	Financial liquidity	33%
8.	Fraud	30%
9.	Organizational culture	26%
10.	Market changes	26%
11.	Communications/reputation	22%
12.	**Climate change**	**22%**
13.	Governance/corporate reporting	18%
14.	Supply chain and outsourcing	16%
15.	Health and safety	8%
16.	Mergers and acquisitions	3%

What are the top 5 risks your organization will face 3 years from now?

1.	Cybersecurity	69%
2.	**Digital disruption**	**56%**
3.	Human capital	43%
4.	Business continuity	43%
5.	**Climate change**	**41%**
6.	Regulatory change	40%
7.	Geopolitical uncertainty	40%
8.	Market changes	28%
9.	Fraud	27%
10.	Financial liquidity	25%
11.	Organizational culture	21%
12.	Governance/corporate reporting	17%
13.	Communications/reputation	15%
14.	Supply chain and outsourcing	15%
15.	Health and safety	11%
16.	Mergers and acquisitions	9%

Note: The IIA's Risk in Focus Global Survey, Latin America, *n* = 956. Percentage who ranked the area as one of their organization's top 5 highest risks.

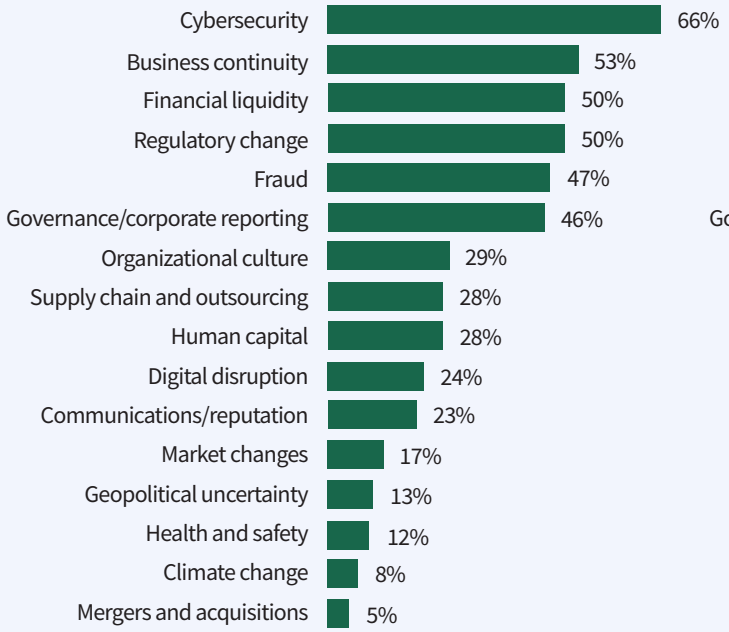
Figure 7:

Current audit effort vs. future audit effort – Latin America

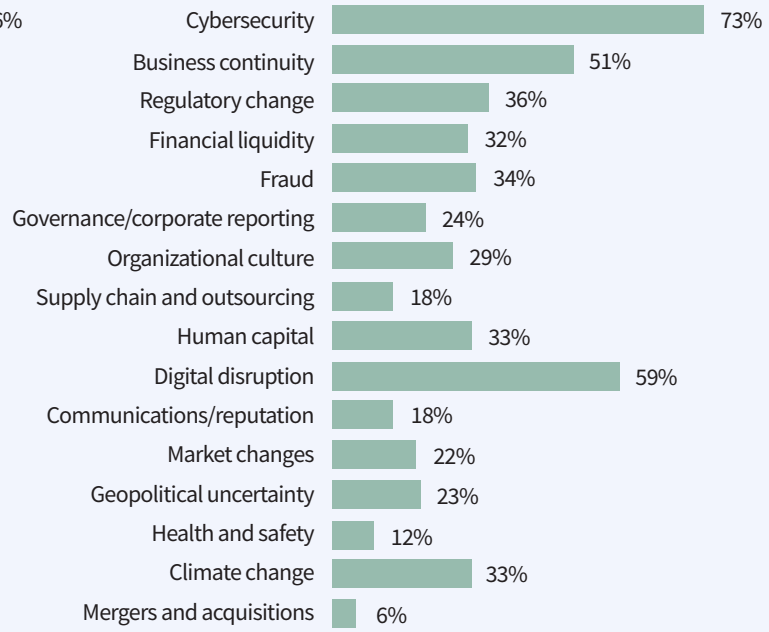
Current effort
Future effort

- Latin American CAEs were most likely to choose cybersecurity as one of their top 5 areas for internal audit effort (67%).
- A wide variety of areas followed close behind cybersecurity, including business continuity, financial liquidity, and regulatory change.

What are the top 5 risks on which internal audit spends the most time and effort?



What are the top 5 risks you expect internal audit to spend the most time and effort addressing 3 years from now?



Note: The IIA's Risk in Focus Global Survey, Latin America, *n* = 956. Percentage who ranked the area as one of their top 5 for audit time and effort.

Figure 8:

Expected audit effort change in 3 years – Latin America

Expected effort change

- Steep rises are expected for activity to deal with digital disruption and climate change.
- Increases are offset by reductions for financial liquidity, regulatory change, and fraud.

What are the top 5 risks on which internal audit spends the most time and effort?

1.	Cybersecurity	66%
2.	Business continuity	53%
3.	Financial liquidity	50%
4.	Regulatory change	50%
5.	Fraud	47%
6.	Governance/corporate reporting	46%
7.	Organizational culture	29%
8.	Supply chain and outsourcing	28%
9.	Human capital	28%
10.	**Digital disruption**	**24%**
11.	Communications/reputation	23%
12.	Market changes	17%
13.	Geopolitical uncertainty	13%
14.	Health and safety	12%
15.	**Climate change**	**8%**
16.	Mergers and acquisitions	5%

What are the top 5 risks you expect internal audit to spend the most time and effort addressing 3 years from now?

1.	Cybersecurity	73%
2.	**Digital disruption**	**59%**
3.	Business continuity	51%
4.	Regulatory change	36%
5.	Fraud	34%
6.	**Climate change**	**33%**
7.	Human capital	33%
8.	Financial liquidity	32%
9.	Organizational culture	29%
10.	Governance/corporate reporting	24%
11.	Geopolitical uncertainty	23%
12.	Market changes	22%
13.	Communications/reputation	18%
14.	Supply chain and outsourcing	18%
15.	Health and safety	12%
16.	Mergers and acquisitions	6%

Note: The IIA's Risk in Focus Global Survey, Latin America, *n* = 956. Percentage who ranked the area as one of their top 5 for audit time and effort.

Figure 9:

Current risk levels vs. current audit effort – Latin America

- Effort is relatively high compared to risk for financial liquidity, fraud, and governance/corporate reporting.
- Effort is relatively low compared to risk for geopolitical uncertainty, market changes, and climate change, but audit effort to address these may cross over other areas.

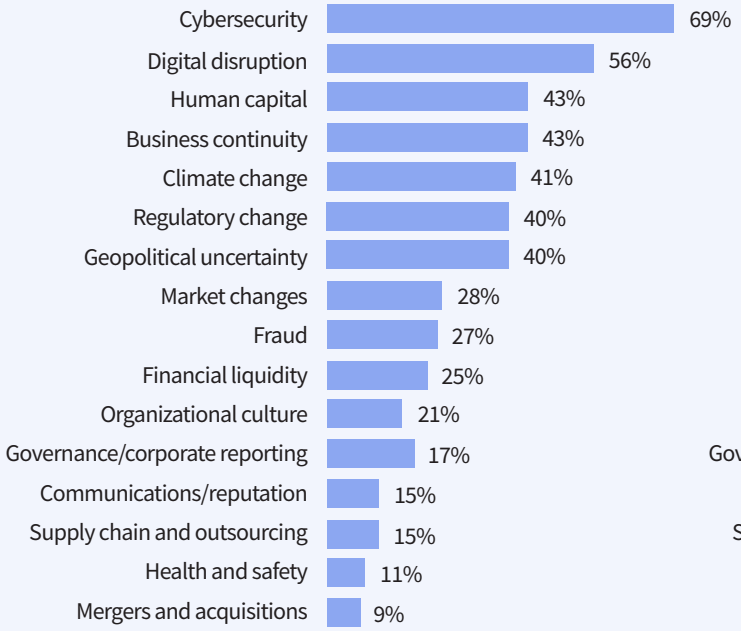
Note: The IIA's Risk in Focus Global Survey, Latin America, *n* = 956. Percentage who ranked the area as one of their top 5 for risk or internal audit effort.

Figure 10:

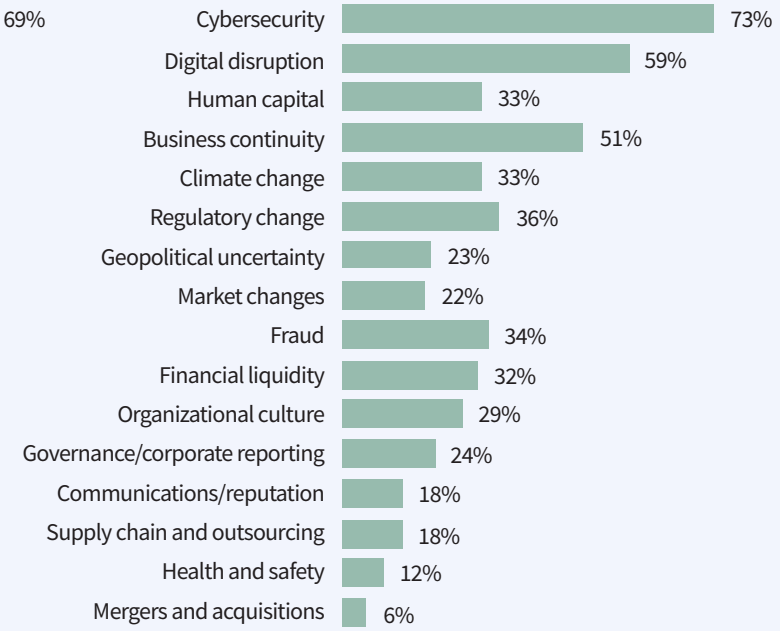
Future risk levels vs. future audit effort – Latin America

- In 3 years, CAEs expect the gap between key risks and the internal audit effort to narrow in most areas.
- Cybersecurity and digital disruption are expected to share top billing for both risk and audit effort.

What are the top 5 risks your organization will face 3 years from now?



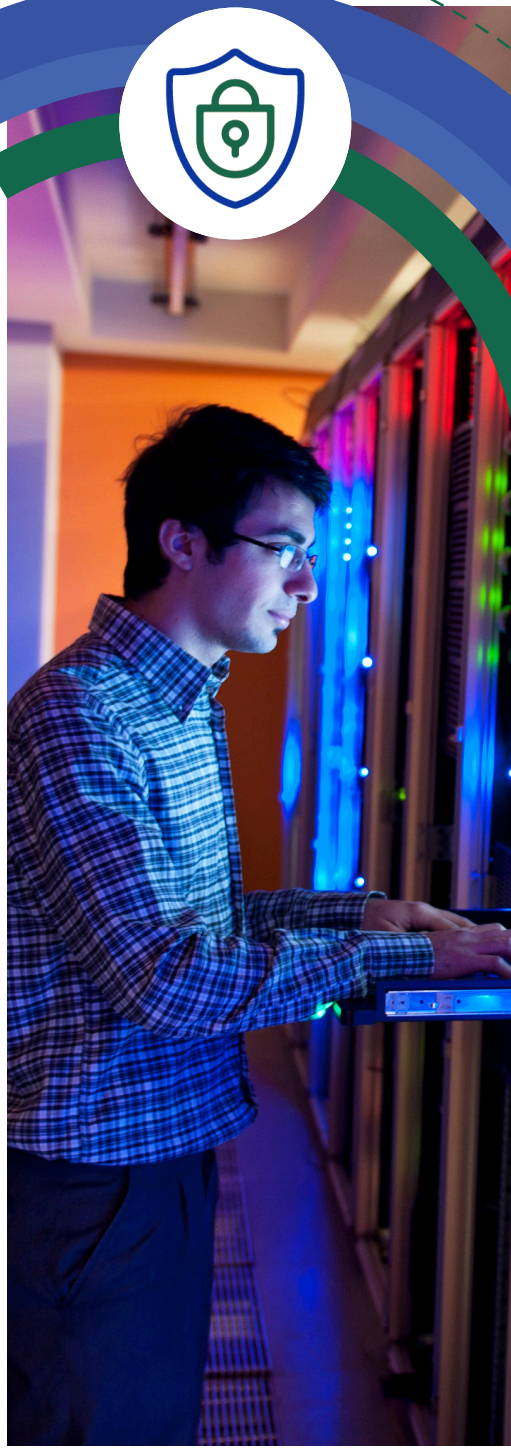
What are the top 5 risks you expect internal audit to spend the most time and effort addressing 3 years from now?



Note: The IIA's Risk in Focus Global Survey, Latin America, *n* = 956. Percentage who ranked the area as one of their top 5 for risk or internal audit effort.

CYBERSECURITY

Pulling together on cybersecurity



With relatively low levels of cybersecurity and data security regulation, CAEs are building resilience by creating relationships inside the business and with other organizations in the region.

Cloud services have boomed in Latin America over the past few years, fueled by the pandemic. One study found that compound growth in the use of cloud services was 22.4% between 2019 and 2023.[1] CAEs at the roundtable said organizations too often implement new cloud services before the proper controls and training are in place. In addition, some complained that businesses were unable to do thorough due diligence on some third-party services, or insist on right-to-audit clauses, because of the ability of powerful businesses to refuse.

Lagging regulations hinder risk response

Hacking has become commonplace in the region, as such third-party connections often introduce vulnerabilities. IBM said that Brazil accounted for the most cases that they responded to in 2023, followed distantly by Colombia and Mexico. The industries favored by hackers were retail-wholesale, finance and insurance, and energy.[2]

Survey Results – Cybersecurity

1ST – RISK LEVEL
75% ranked it as a top 5 *for risk level*

1ST – AUDIT EFFORT
66% ranked it as a top 5 *for audit effort*

[1] For more about global cloud computing activity, see https://aag-it.com/the-latest-cloud-computing-statistics/
[2] For more about worldwide threats, see the IBM Security X-Force Threat Intelligence Index 2023 at https://www.ibm.com/reports/threat-intelligence

CYBERSECURITY

A CAE at a Bolivian bank said the lack of specific cybersecurity regulations hinders effective defense across the region. Cybersecurity regulations would mandate minimum cybersecurity procedures and processes and come with recommended control frameworks, governance best practices, and, sometimes, non-compliance penalties. Government regulations could also establish a system for alerting organizations about new cyber threats. Without such a system, he said, organizations often do not have effective information-sharing relationships. “Since we do not share information about cybersecurity attacks, we are blind,” he said.

CAEs agreed they cannot wait for regulations to be put in place, especially in fast-moving areas such as AI (artificial intelligence). As a result, organizations are using internationally recognized frameworks, such as NIST, to combat the threat.[3] A CAE at a financial services business in Panama was positive about his NIST experience, “Our analysis showed where we stood on the maturity level compared to other businesses, what responses we needed to make to close the gaps, and provided a roadmap to get there.”

Relationships strengthen defenses

Internal audit functions are investing in boosting knowledge and keeping up to date in disruptive technologies, such as AI, where the business may be eager to implement software. “We decided to block Open AI,” said Pamela Vago, CAE at Genneia, an energy company in Argentina. “It is part of our company ethic to train people before using these technologies to make sure they understand what company information they can use and what they cannot disclose.”

She said it is key for CAEs to build relationships with the business lines that are introducing new technologies so that internal audit can provide strategic advice on risk and controls ahead of implementation. Being in close touch with frontline management can also help identify potential weak points.

“We allocate our research efforts to where the risk is highest, and if we see that the risk is not being managed somewhere in the company, we need to bring it to the leaders and ensure an action plan is put in place to mitigate it,” she said.

That approach can be difficult where enterprises operate in several countries either in South America or further afield. Cyber maturity is often uneven – hampered in countries with fewer resources. A CAE at a Bolivian bank said he had created a corporate internal audit program to standardize knowledge across the business’s different regions. “We share experience between all the auditors in the corporation,” he said, “and we have created committees of specialists, too, to share the problems we identify in all of the countries in which we operate.”

[3] For more about the NIST framework, see https://www.nist.gov/cybersecurity

CYBERSECURITY

Risk velocity met by reconfiguring governance

Given the velocity and ferocity of the cyber risk landscape, CAEs at the roundtable said that some effective strategies are:

- Reconfiguring governance structures to enable better combined assurance between the three lines.
- Creating additional enterprise-wide risk committees dedicated to the threat.
- Boosting audit committees and boards by mandating at least one non-executive director have a specialty in cybersecurity.

A CAE at a Brazilian bank said he had made IT responsible for cyber risk and effectively included it in the governance system as a fourth line. “This has been super healthy for the organization and has created a lot of value,” he said.

Cyber defense requires knowledge

Awareness of cyberattacks is high, but so are talent shortages for key IT and cyber skills. Most internal audit functions would benefit from a cybersecurity expert, but positions are difficult to fill or too expensive. Given these challenges, training and awareness have become the focus, CAEs at the roundtable agreed. CAEs are encouraging auditors to become certified in IT areas.

While creating a cyber-secure culture has been made more difficult by higher staff turnover during and following the pandemic, CAEs at the roundtable said they were leveraging online training to share resources and knowledge. Some also said they use their relationships with operational IT providers to provide updates and training for free. Where staff have been trained, they are sometimes asked to pass that knowledge along to others in the business.

Resources

Assessing Cybersecurity Operations: Prevention and Detection (The IIA)

The IIA’s Three Lines Model

Three Lines Model explains the roles of the first, second, and third lines in governance.

“We are doing a lot more training to make everyone in the organization more aware because if people do not have the knowledge of how phishing attacks work, it is very easy for hackers to break into the company,” said José Gabriel Calderón, CAE at the Mexican multinational food company Grupo Bimbo.

CYBERSECURITY

How internal audit can help the organization

1. Include cybersecurity audits in the audit plan on a recurring basis and report the results to the board of directors and executive management.
2. If regional cybersecurity regulations are weak or non-existent, encourage the organization to use alternative cybersecurity frameworks, such as NIST.
3. Evaluate how well management understands disruptive technologies, such as AI, before implementing them, and build relationships within the organization so you can provide input on emerging risks.
4. Assess the effectiveness of governance structures to help optimize collaboration between the three lines on cybersecurity and data security.
5. Evaluate the cybersecurity training and awareness programs and how well such campaigns are disseminated throughout the organization.

BUSINESS CONTINUITY

Connecting for improved resilience

In a dynamic, inter-connected risk landscape, teamwork and acting rapidly and decisively is key to recovering after impairment or shutdown of operations.

While operational failure is a major threat in itself, the reasons behind it are connected with other top risks facing organizations in Latin America. Ransomware attacks, unexpected changes to laws and regulations, as well as macroeconomic uncertainty, climate change, and supply chain failures create a complex, inter-locking array of risks that can cause partial or total shutdowns of business operations.

Political tensions in the region can trigger unexpected changes in the business sector, CAEs at the roundtable said. For example, the Nicaraguan government nationalized a major gas station company in 2023 in apparent retaliation against U.S. sanctions, creating major challenges for other businesses and organizations.[4] Argentina, Brazil, Chile, Colombia, Mexico, and Peru all face potential strikes and political unrest in 2023, which further threatens business continuity.[5] And elections in several countries are creating further political uncertainty.

Survey Results – Business Continuity

3RD – RISK LEVEL
47% ranked it as a top 5 *for risk level*

2ND – AUDIT EFFORT
53% ranked it as a top 5 *for audit effort*

[4] For more about the nationalization of the gas station company, see https://www.reuters.com/article/us-nicaragua-ortega-idUSKBN1YI0LV

[5] For more about political unrest in Latin America, see https://www.lexology.com/library/detail.aspx?g=17706d05-173b-474a-a928-97ab1385493d

BUSINESS CONTINUITY

Business continuity is grounded in relationships

The pandemic helped to build key relationships needed to respond to crises – while at the same time raising awareness that business continuity planning is essential.

A CAE from the airline industry in El Salvador said that her company was able to keep flights going during the pandemic due to cooperation and dialogue with the national government. The impact of COVID underscored the necessity of planning for unlikely events. "The episode changed the mindset of senior management, who had always delayed internal audit's recommendations to create disaster recovery plans," she said. "COVID helped them understand that those risks that are very unlikely to happen can be catastrophic when they do."

Where disaster recovery exercises have strengthened the relationship between internal audit and management, the two groups are more likely to work together to launch a rapid response the moment strategic goals are threatened. For example, when Panama closed its borders to certain imported goods, breaking established supply chains, exports were affected overnight. A CAE at a Costa Rican dairy producer, whose business was affected by the event, said management turned to internal audit to help the business scope out new manufacturing arrangements in Panama itself – and operations were resumed.

Disaster response plans need to be agreed upon by internal audit and management. "In any business continuity plan, you need to have clear support from top management to ensure they are going to buy into the project, otherwise you are only going to be dealing with things at an operational level," said Fábio Pimpão, director of internal audit at Whirlpool Latin America. Once secured, each plan must be detailed enough to capture all potential variables (including inter-connected risks) and also be well-documented and thoroughly tested, he said. That includes paying close attention to critical supply chain infrastructure.

"COVID helped them understand that those risks that are very unlikely to happen can be catastrophic when they do."

BUSINESS CONTINUITY

Embed controls throughout operations

To achieve operational resilience, business continuity should be embedded into every aspect of an organization's operations, and impact analyses and risk assessments need to be kept up to date. CAEs at the roundtable said internal audit must cover both emerging risks, such as blockchain and AI, as well as those that have existed for many years, such as political instability, fraud, and regulatory risk. It can be tempting to only focus on new and emerging threats, but fallout from well-known risks can also knock out operations. Continually advocating the need for business continuity planning is essential to prevent senior management from falling back into pre-pandemic complacent thinking.

In fast-moving areas such as cybersecurity, CAEs must be aware of cutting-edge cyberattack methodologies, said CAEs at the roundtable, with cyber risk assessments, controls testing, and active monitoring being a part of every assignment. Working closely with IT and the risk management function is essential, and, since social engineering attacks depend on a lack of awareness among staff, training is critical. "We do not just facilitate training, we attend it as well," said a CAE at a financial firm in Guatemala, "because we need to be aware of what is happening."

High-quality enterprise risk management (ERM) is foundational for all business continuity and operational resilience plans. "Effective business continuity has to be collaborative and has to be based on solid and sound ERM," a CAE from a Peruvian mining company said, "I joke with the board that if I were to do only one audit per year, I would audit ERM."

Diverse teams create better resilience

Given the wide range of risks that feed into internal audit's work on business continuity, acquiring the right balance of skills is extremely difficult. In three years, survey respondents said they expected digital disruption to move into second place as a key risk, and climate change to jump to fifth place (see Figure 6). CAEs said they were seeking to diversify their teams early to be ready for these challenges, despite shortages in technical skills, particularly for small audit functions and the public sector.

Resources

Auditing Third-Party Risk Management (The IIA)

Business Continuity Management (The IIA)

BUSINESS CONTINUITY

How internal audit can help the organization

1. Build relationships with executive management and the audit committee and work together to improve the development and testing of business continuity plans.
2. Assess how well business continuity plans have been documented and tested.
3. Evaluate whether the organization's knowledge of its key risks is up to date and covers the entire risk universe – rather than being overly focused on emerging risks.
4. Assess the organization's future human capital requirements based on business continuity planning results.
5. As appropriate, include an audit of the organization's continuity plans in the audit plan.

GEOPOLITICAL UNCERTAINTY

Planning for widespread impacts of change

Political uncertainty has increased the risk of regulatory change in some countries, but CAEs are making sure these problems are on their organizations' risk agendas.

Political disruption has been a feature in many Latin American countries in recent years as voters head to the polls in Argentina, Guatemala, and Paraguay. It is part of a so-called super-cycle, which runs from 2021 to 2024 and sees elections in all of the region's countries.[6]

"Political disruption as governments change is significantly affecting business liquidity, and inflation is impacting local markets," a CAE at a Guatemalan financial institution explained.

Some countries in the region may experience government changes that alter economic policies or restrict economic activity. CAEs can help boards prepare for political changes that could put their business at risk by helping to find alternative plans to enable the continuity of their business in the long-term and seeking out expert support, such as legal and foreign trade specialists.

Survey Results – Geopolitical Uncertainty

5TH – RISK LEVEL

42% ranked it as a top 5 *for risk level*

13TH – AUDIT EFFORT

13% ranked it as a top 5 *for audit effort*

[6] For more about Latin America politics from IDEA, see https://www.idea.int/news-media/news/latin-america-political-and-electoral-outlook-2023

Contents

GEOPOLITICAL UNCERTAINTY

Plan ahead to prevent cash flow crisis

Changes to laws and regulations can be large-scale, fast, and impactful, CAEs at the roundtable agreed.

"Internal auditors must be well-informed about political changes, or changes to laws and regulations," said Francisco Ramón Aráuz Rodríguez, president of Fundación Latinoamericana de Auditores Internos (FLAI). "CAEs must be able to alert their organizations in a timely manner, evaluating and determining the impact of such events and rules."

The goal is for the CAE to work in partnership with the audit committee to discuss how political and economic environment events could impact the business and react accordingly, he said. In addition, CAEs should proactively monitor emerging risks and their impacts on customers and supply chains and assess how they interact.

"Politics, the environment, trade barriers, macroeconomic risks – you need to combine these threats and have a holistic view so that you can advise management how they should act," said Fábio Pimpão, director of internal audit at Whirlpool Latin America. In particular, CAEs should create scenarios and simulations to better understand the inter-relationships between the risks and have a plan in place before crisis comes.

Such scenarios can provide CAEs with potential strategic and operational audit themes, as well as aid in identifying areas where insurance is needed, opportunities for governance improvements across the enterprise, and ways to ensure the business does not run out of money if a crunch comes. Pimpão explained, "In the end, what is going to break a company is not the P&L account, not its results or reporting failures – it is going to be cash flow," adding, "Scenarios of emerging risk can help determine when internal audit needs to focus on cash management, for instance, to give some strategic recommendations that aid corporate decision making to avert disaster."

GEOPOLITICAL UNCERTAINTY

Push back against money laundering

While political leadership may change rapidly, asset laundering, money laundering, and fraud are deeply engrained problems in many of the region's countries. "Money laundering is perceived as an issue that is all around us," said José Lago Rodríguez, vice president of FLAI.

Many organizations in Latin America do not have detailed anti-money-laundering compliance procedures in place. In general, procedures are only in place for financial services companies, publicly traded organizations, and global companies. Where procedures are lacking, the CAE should consider creating a risk taxonomy that includes asset laundering, money laundering, and fraud; and then map the risks across the enterprise.

CAEs must be aware of the differences in anti-money-laundering compliance requirements from country to country and ensure appropriate control procedures are in place. In recent years, the Latin American Financial Action Group has been developing resources to help organizations in the region navigate the maze of regulatory requirements.[7]

In small teams where the remit of internal audit is narrowly drawn, the CAE may also have the task of educating and persuading the board that internal audit can add value through addressing risks related to money laundering.

Countries such as Argentina have also introduced specific measures to help businesses improve the maturity of their anti-corruption and fraud processes, and internal auditors are helping with their integration, said Pamela Vago, CAE at Genneia, an energy company in Argentina.[8] "We have been working with the company to develop procedures and training for the new laws."

"In the end, what is going to break a company is not the P&L account, not its results or reporting failures – it is going to be cash flow."

[7] For more about efforts against money laundering in Latin America, see https://latinlawyer.com/guide/the-guide-corporate-compliance/second-edition/article/17-anti-money-laundering-and-counter-terrorist-financing-in-latin-america

[8] For more about Argentina's efforts against corruption, see https://www.globalcompliancenews.com/2023/01/06/https-insightplus-bakermckenzie-com-bm-investigations-compliance-ethics-argentina-the-registry-of-integrity-and-transparency-of-companies-and-entities-finally-launched_01042023/

GEOPOLITICAL UNCERTAINTY

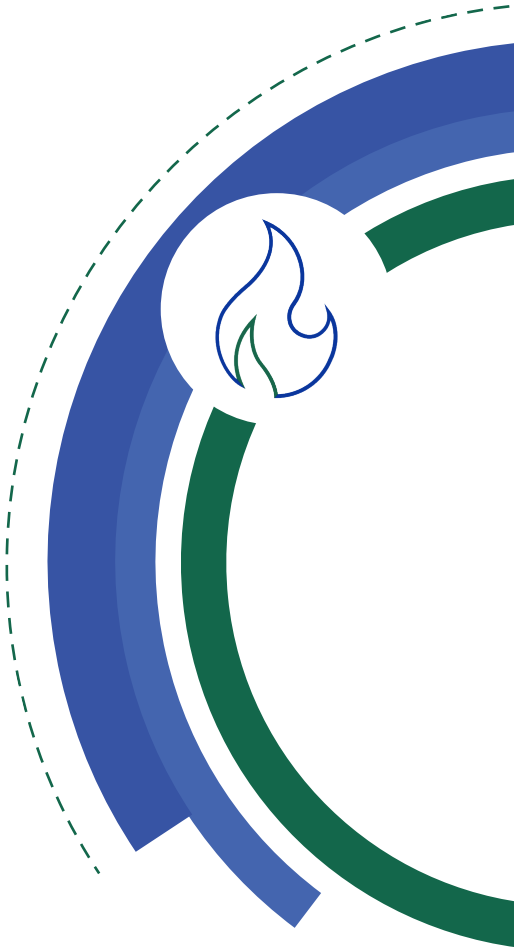
Internal audit provides assurance around governance processes, policies, and the segregation of duties that are established to prevent fraud. While hard controls are important, soft controls – such as an ethics code, hotlines, and complaints procedures – can also help, as long as they are trusted. "There may be a fear of reprisal if you speak up, so employees must be able to trust that the people managing the hotline are not complicit with fraud," said Vago.

As people in many countries struggle with higher prices, organizations will need to have controls in place to reduce temptation to misappropriate funds or assets. "Some areas may not be material – such as petty cash in a large company – but the active presence of the internal audit function can discourage people from committing fraud," Vago said.

While hard controls are important, soft controls – such as an ethics code, hotlines, and complaints procedures – can also help, as long as they are trusted.

Increasing coordination between countries

Slowing growth, higher inflation, and a cost-of-living crunch have put pressure on governments to act – but corruption and weak institutions make it difficult to tackle social problems across the region. Multiple efforts have been made to foster increased integration between South American countries, most recently in May 2023 at a meeting led by the president of Brazil, with hopes of fostering political and economic stability in a region that collectively represents the fifth-largest global economy.[9]



[9] For more about Latin America seeking integration, see https://www.aljazeera.com/news/2023/6/3/south-america-a-hard-road-to-unity

GEOPOLITICAL UNCERTAINTY

How internal audit can help the organization

1. Be aware of impact to the business if a political change brings in a government that restricts economic activities.
2. Prepare for any political changes that could put the business at risk by helping to find alternative plans to enable long-term continuity and seeking out expert support, such as legal and foreign trade specialists.
3. Evaluate the organization's scenario and simulation processes for emerging risks and how well they inform the internal audit plan.
4. Assess whether the organization has the right anti-money-laundering processes in place to comply with regulations and that risks are mapped across the enterprise.
5. Evaluate the business's soft controls around fraud prevention and detection.
6. Review the creation of documents, such as the code of ethics, which should have strong support from the board, executive management, and CAE.

INTERNAL AUDIT FOUNDATION ACKNOWLEDGMENTS

Risk in Focus Development Team

Project directors
Laura LeBlanc –
Senior Director, Internal Audit Foundation
Deborah Poulalion –
Senior Manager, Research and Insights, The IIA
Emely Katz –
Director, Affiliate Engagement, The IIA

Survey analysis and content development
Deborah Poulalion –
Senior Manager, Research and Insights, The IIA

Research writer
Arthur Piper – Smith de Wint, United Kingdom

Graphic designer
Cathy Watanabe

Internal Audit Foundation 2023–24 Board of Trustees

President
Warren W. Stippich Jr., CIA, CRMA

Senior Vice President – Strategy
Glenn Ho, CIA, CRMA

Vice President – Finance and Development
Sarah Fedele, CIA, CRMA

Vice President – Content
Yulia Gurman, CIA

Trustees
Hossam El Shaffei, CCSA, CRMA
Reyes Fuentes Ortea, CIA, CCSA, CRMA
Nora Kelani, CIA, CRMA
Shirley Livhuwani Machaba, CCSA, CRMA
Raoul Ménès, CIA, CCSA, CRMA
Hiroshi Naka, CIA
Anthony J. Pugliese, CIA
Bhaskar Subramanian

Staff liaison
Laura LeBlanc –
Senior Director, Internal Audit Foundation

Internal Audit Foundation 2023–24 Committee of Research and Education Advisors

Chair
Yulia Gurman, CIA

Vice-Chair
Jane Traub, CIA, CCSA, CRMA

Members
Tonya Arnold-Tornquist, CIA, CRMA
Christopher Calvin, CIA
Jiin-Feng Chen, CIA
Andre Domingos
Christina Duquette, CRMA
Marc Eulerich, CIA
Dagmar Flores, CIA, CCSA, CRMA
Anargul Kairulla, CIA
Ayaka Mitsunari
Ahmed Mohammed, CIA
Grace Mubako, CIA
Ruth Doreen Mutebe, CIA
Erika C. Ray, CIA
Brian Tremblay, CIA
Koji Watanabe

Staff liaison
Deborah Poulalion –
Senior Manager, Research and Insights, The IIA

FUNDACIÓN LATINOAMERICANA DE AUDITORES INTERNOS (FLAI)

Board of Directors, 2021-24

President
Francisco Ramón Aráuz Rodríguez, CIA, CCSA

Vice President
José Lago Rodríguez, CIA, CFSA

Secretary
Gabriel Benavides

Treasurer
Máximo Perdomo, CIA

Directors
Renato Trisciuzzi, CIA , QIAL, CRMA, CCSA
Maritza Barzola

Latin America Report Development Team

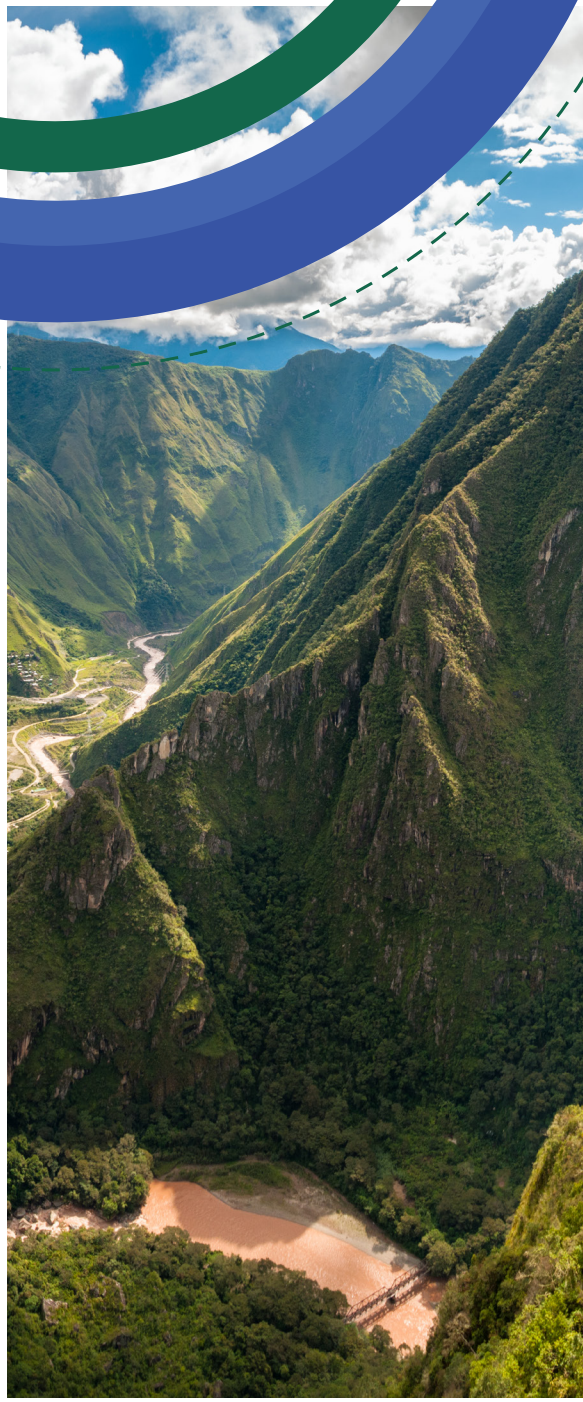
Regional liaisons
Roberto Loo, Executive Director, Fundación Latinoamericana de Auditores Internos

Jorge Badillo Ayala, CIA, QIAL, CCSA, CGAP, CRMA, CFE, CISA – Director, Global Services (IRC) IIA Global

Roundtable moderators
Fábio Pimpão, Director, Internal Audit, Whirlpool Latin America

José Gabriel Calderón, CAE, Grupo Bimbo

Translations sponsor
Grupo Bimbo
(Corporativo Bimbo, S.A. de C.V.)



SPONSORS

FOUNDATION STRATEGIC PARTNERS

ARABCIIA
الاتحاد العربي لجمعيات المراجعين الداخليين
Arab Confederation for Institutes of Internal Auditors

AUDITBOARD

Deloitte.

Grant Thornton

The Institute of Internal Auditors
Chicago

The Institute of Internal Auditors

Foundation Partners

African Federation of Institutes of Internal Auditors

Asian Confederation of Institutes of Internal Auditors

Crowe

European Confederation of Institutes of Internal Auditing

Fundación Latinoamericana de Auditores Internos

Gold Partners

Larry Harrington
CIA, QIAL, CRMA

Stacey Schabel
CIA

The Institute of Internal Auditors
Houston

The Institute of Internal Auditors
Japan

南京審計大學
NANJING AUDIT UNIVERSITY

The Institute of Internal Auditors
New York

The Institute of Internal Auditors
San Francisco

RISK IN FOCUS PARTNERS

IIA – Argentina
IIA – Australia
IIA – Bolivia
IIA – Brazil
IIA – Chile
IIA – Colombia
IIA – Costa Rica
IIA – Dominican Republic
IIA – Ecuador
IIA – El Salvador
IIA – Ghana
IIA – Guatemala
IIA – Hong Kong
IIA – Indonesia
IIA – Japan
IIA – Kenya
IIA – Malaysia
IIA – Mexico
IIA – Nicaragua
IIA – Panama
IIA – Paraguay
IIA – Peru
IIA – Philippines
IIA – Rwanda
IIA – Singapore
IIA – South Africa
IIA – Tanzania
IIA – Uganda
IIA – Uruguay
IIA – Venezuela

ABOUT THE IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 235,000 global members and has awarded more than 190,000 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.

About the Internal Audit Foundation

The Internal Audit Foundation provides insight to internal audit practitioners and their stakeholders, promoting and advancing the value of the internal audit profession globally. Through the Academic Fund, the Foundation supports the future of the profession through grants to support internal audit education at institutions of higher education. For more information, visit theiia.org/Foundation.

Disclaimer and Copyright

Internal Audit
FOUNDATION

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