
2024
RISK IN FOCUS
Hot topics for internal auditors
AFRICA
Read more
Internal Audit FOUNDATION
African Federation of Institutes of Internal Auditors

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.

Each of The IIA's six regions will receive two reports:

- **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).

AFRICA REPORT SPONSORS

African Federation of Institutes of Internal Auditors

IIA–Democratic Republic of the Congo
IIA–Ghana
IIA–Kenya
IIA–Rwanda
IIA–South Africa
IIA–Tanzania
IIA–Uganda
IIA–Zambia

CONTENTS

Contents

EXECUTIVE SUMMARY – AFRICA
Africa's digital revolution

Africa is rapidly embracing a digital revolution to improve government services and to meet customer demands for mobile and online services. But achieving those strategies is fraught with difficulties – including sophisticated cyberattacks against organizations and cyber fraud aimed at new technology users.

Africa 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?

While Africa is similar to most respondents worldwide in having cybersecurity and business continuity as its two highest risk areas in 2024, Africa was unique in also having financial liquidity and fraud in its top 5. In terms of internal audit activity, CAEs allocated the most effort in 2024 to addressing fraud and business continuity.

In the next three years, CAEs in Africa expect digital disruption and climate change to be the fastest climbing risks for their organizations, both of which will also see significant increases in internal audit effort. This is consistent with responses from CAEs worldwide.

Based on highest risk and internal audit effort, the featured topics for the Africa Risk in Focus reports are:

Cybersecurity – CAEs are supporting efforts to automate processes that prevent, detect, and monitor cyber threats.

Fraud – Fraudsters have been quick to exploit control weaknesses in digital systems and low levels of cyber fraud awareness among the public.

Africa Research Participation

- **808 survey responses** from CAEs and directors
- **28 participating countries/territories**
- **2 roundtables** with 14 participants
- **5 in-depth interviews**

Contents

EXECUTIVE SUMMARY – AFRICA

Business continuity – CAEs are supporting stronger governance processes and turning to data analytics to improve their organizations' business continuity planning.

Digital disruption and climate change – Internal auditors in Africa are adapting to the new realities of these rapidly growing risk areas.

The Africa Risk in Focus reports describe in detail the challenges and solutions for urgent risk areas and draw on the expertise, experience, and knowledge of multiple internal audit leaders throughout the region.

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

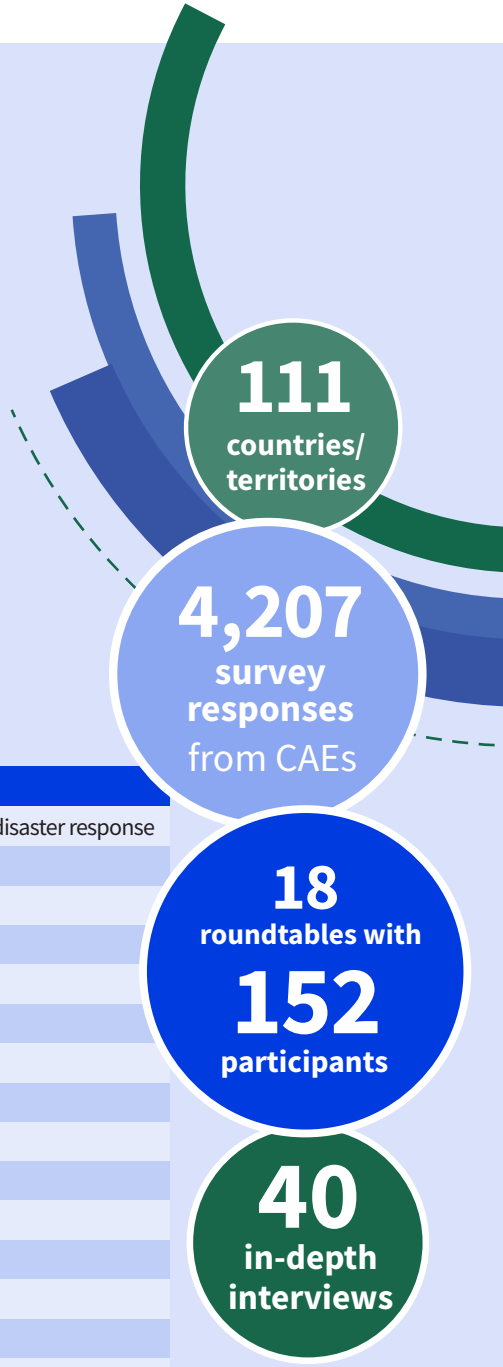
Contents

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 are summarized below, 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.

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

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

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:

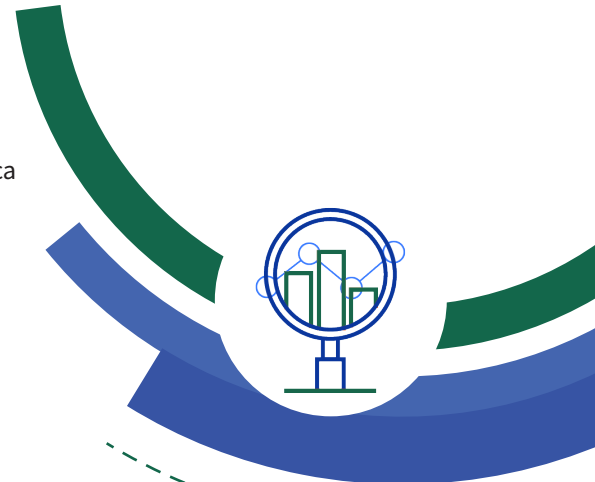
1. Cybersecurity
2. Governance/corporate reporting
3. Business continuity
4. Regulatory change
5. Financial liquidity
6. Fraud

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.

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

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).



Contents

SURVEY RESULTS – GLOBAL

Another 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.

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

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%.

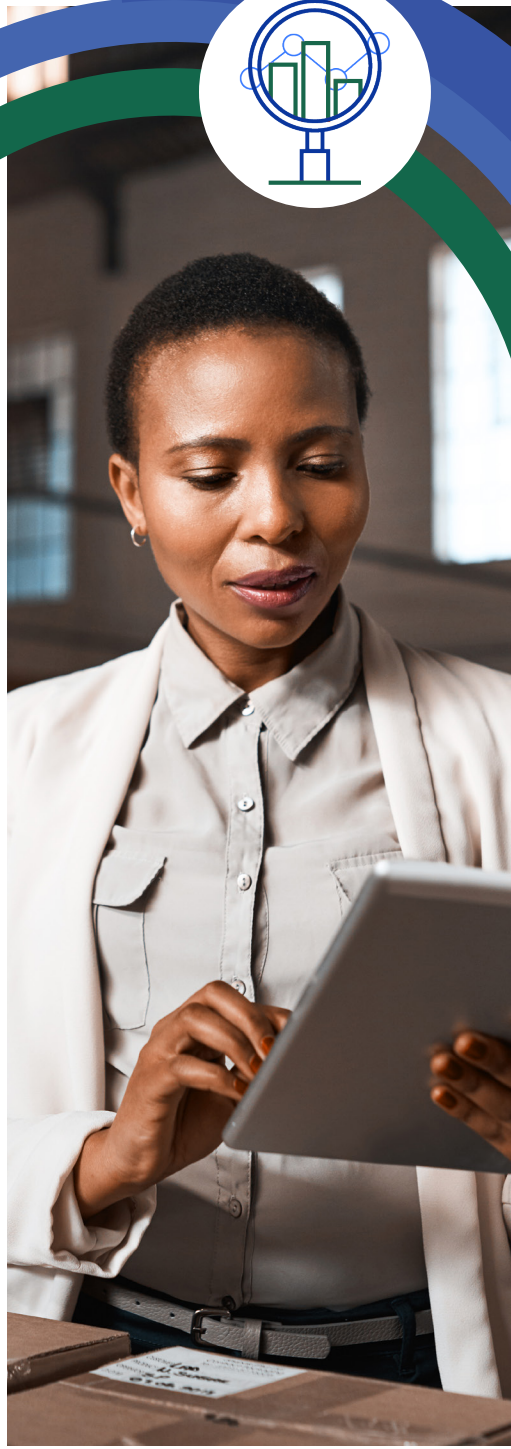


Figure 1:

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 – cybersecurity, governance/corporate reporting, and business continuity.

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 risk increases dramatically to fifth place, up from fourteenth place.

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 – AFRICA

How to use survey results

Key findings for Africa 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. 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 5: Current risk levels vs. future risk levels

- More than half of respondents in Africa said cybersecurity and business continuity are top 5 risks.
- In the next three years, risk levels for financial liquidity and fraud are expected to decrease, while digital disruption and climate change risks increase.

Figure 6: Expected risk change in three years

- Digital disruption is expected to move to second place, with 53% saying it will be a top 5 risk.
- Climate-related risk leaps into fifth position, with 35% saying it will be a top 5 risk.

Figure 7: Current audit effort vs. future audit effort

- Fraud currently holds the top rank for internal audit time and effort, but three years from now, it's expected to drop to fourth.
- Cybersecurity and digital disruption are expected to rise to first and second place.

Africa Survey Responses Per Country

Kenya	168	Mauritius	10	Mali	4
Tanzania	142	Nigeria	9	Botswana	3
Uganda	102	Tunisia	9	Ethiopia	3
Ghana	68	Namibia	8	Cote d'Ivoire	2
Zimbabwe	65	Morocco	7	South Sudan	2
South Africa	55	Zambia	7	Sudan	2
Malawi	52	Democratic Republic		Benin	1
Rwanda	27	of the Congo	5	Burkina Faso	1
Senegal	24	Lesotho	5	Congo	1
Angola	22	Eswatini	4	**TOTAL**	**808**

SURVEY RESULTS – AFRICA

Figure 8: Expected audit effort change in three years

- Steep rises are expected for internal audit activity to deal with digital disruption and climate change.
- Fraud, financial liquidity, and governance/corporate reporting are expected to become less time-consuming.

Figure 9: Current risk levels vs. current audit effort

- For Africa in particular, risk levels and audit effort are well-aligned, especially for high-risk areas.
- One notable area where risk outweighs current effort is digital disruption, but audit effort is expected to increase in this area significantly in the next three years.

Figure 10: Future risk levels vs. future audit effort

- In three years, cybersecurity and digital disruption are expected to share top billing for both risk and audit effort.
- Risk and audit effort are expected to continue to be well-balanced for the Africa region.

Figure 5:

Current risk levels vs. future risk levels – Africa

- More than half of respondents in Africa said cybersecurity and business continuity are top 5 risks.
- In the next three years, risk levels for financial liquidity and fraud are expected to decrease, while digital disruption and climate change risks increase.

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, Africa, *n* = 808. Percentage who ranked the area as one of their organization's top 5 highest risks.

Figure 6:

Expected risk change in 3 years – Africa

Expected risk change

- Digital disruption is expected to move to second place, with 53% saying it will be a top 5 risk.
- Climate-related risk leaps into fifth position, with 35% saying it will be a top 5 risk.

What are the top 5 risks your organization currently faces?

1.	Cybersecurity	58%
2.	Business continuity	52%
3.	Financial liquidity	47%
4.	Fraud	46%
5.	Human capital	39%
6.	Governance/corporate reporting	36%
7.	Organizational culture	34%
8.	**Digital disruption**	**33%**
9.	Regulatory change	32%
10.	Communications/reputation	27%
11.	Geopolitical uncertainty	25%
12.	Market changes	21%
13.	**Climate change**	**19%**
14.	Supply chain and outsourcing	19%
15.	Health and safety	10%
16.	Mergers and acquisitions	3%

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

1.	Cybersecurity	62%
2.	**Digital disruption**	**53%**
3.	Business continuity	47%
4.	Human capital	38%
5.	**Climate change**	**35%**
6.	Fraud	33%
7.	Regulatory change	32%
8.	Geopolitical uncertainty	31%
9.	Governance/corporate reporting	29%
10.	Financial liquidity	29%
11.	Organizational culture	25%
12.	Market changes	25%
13.	Supply chain and outsourcing	22%
14.	Communications/reputation	19%
15.	Health and safety	13%
16.	Mergers and acquisitions	7%

Note: The IIA's Risk in Focus Global Survey, Africa, *n* = 808. Percentage who ranked the area as one of their organization's top 5 highest risks.

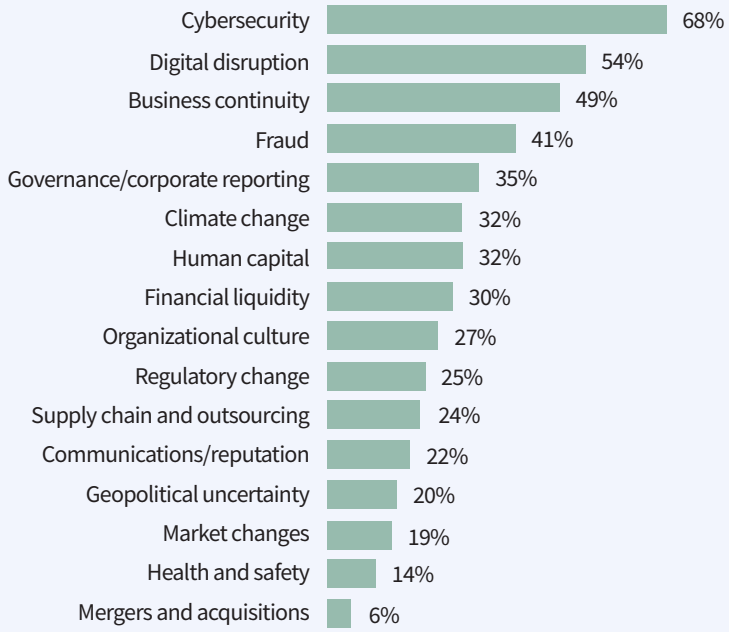
Figure 7:

Current audit effort vs. future audit effort – Africa

- Fraud currently holds the top rank for internal audit time and effort, but three years from now, it is expected to drop to fourth.
- Cybersecurity and digital disruption are expected to rise to first and second place.

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, Africa, *n* = 808. 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 – Africa

Expected effort change

- Steep rises are expected for internal audit activity to deal with digital disruption and climate change.
- Fraud, financial liquidity, and governance/corporate reporting are expected to become less time-consuming.

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

1.	Fraud	57%
2.	Business continuity	56%
3.	Cybersecurity	54%
4.	Financial liquidity	53%
5.	Governance/corporate reporting	52%
6.	Regulatory change	35%
7.	Human capital	33%
8.	Supply chain and outsourcing	32%
9.	Organizational culture	27%
10.	Communications/reputation	25%
11.	**Digital disruption**	**24%**
12.	Market changes	15%
13.	Health and safety	13%
14.	Geopolitical uncertainty	12%
15.	**Climate change**	**11%**
16.	Mergers and acquisitions	2%

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

1.	Cybersecurity	68%
2.	**Digital disruption**	**54%**
3.	Business continuity	49%
4.	Fraud	41%
5.	Governance/corporate reporting	35%
6.	**Climate change**	**32%**
7.	Human capital	32%
8.	Financial liquidity	30%
9.	Organizational culture	27%
10.	Regulatory change	25%
11.	Supply chain and outsourcing	24%
12.	Communications/reputation	22%
13.	Geopolitical uncertainty	20%
14.	Market changes	19%
15.	Health and safety	14%
16.	Mergers and acquisitions	6%

Note: The IIA's Risk in Focus Global Survey, Africa, *n* = 808. 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 – Africa

- For Africa in particular, risk levels and audit effort are well-aligned, especially for high-risk areas.
- One notable area where risk outweighs current effort is digital disruption, but audit effort is expected to increase in this area significantly in the next three years.

What are the top 5 risks your organization currently faces?

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

Note: The IIA's Risk in Focus Global Survey, Africa, *n* = 808. Percentage who ranked the area as one of their top 5 for risk or internal audit effort.

Figure 10:

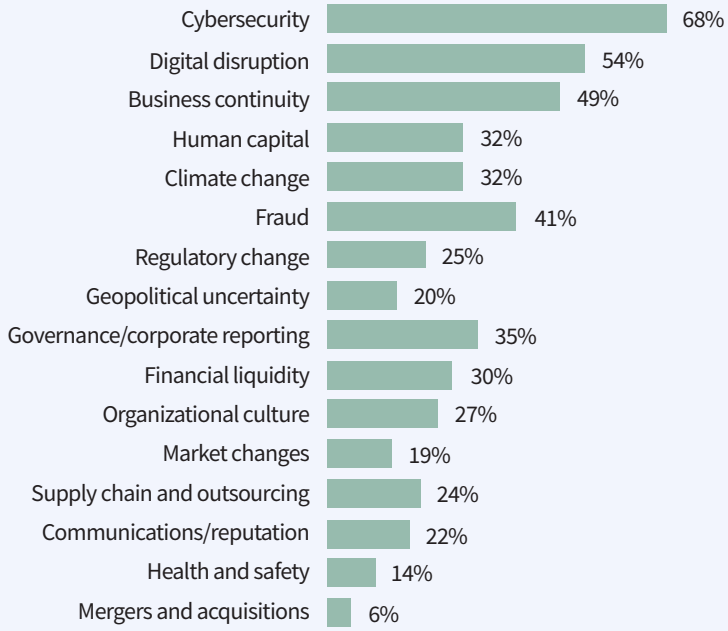
Future risk levels vs. future audit effort – Africa

Future risk
Future effort

- In three years, cybersecurity and digital disruption are expected to share top billing for both risk and audit effort.
- Risk and audit effort are expected to continue to be well-balanced for the Africa region.

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, Africa, *n* = 808. Percentage who ranked the area as one of their top 5 for risk or internal audit effort.

CYBERSECURITY

Building defenses for new technologies

Digitalization efforts have often outstripped cyber maturity within African organizations. CAEs are catching up with cyber criminals by spreading awareness, strengthening technological defenses, and sharing best practices within their businesses.

Digital transformation has accelerated in most African countries over the past couple of years. Fueled by consumer and business demand during the pandemic and backed by national governments and organizations such as the African Union,[1] digital government and commerce have become a reality in most urban centers and are rapidly reaching rural communities.[2]

As Africa's organizations rapidly embrace digitalization, cyberattacks have risen. The most advanced countries technologically have also been the hardest hit – with Kenya, Nigeria, and South Africa becoming the continent's most targeted places.[3] Malware, phishing, and brute force attacks are on the rise. And hackers persistently target government agencies, national infrastructure, and financial services firms, according to CAEs at the Risk in Focus roundtables.

Survey Results – Cybersecurity

1ST – RISK LEVEL
58% ranked it as a top 5 *for risk level*

3RD – AUDIT EFFORT
54% ranked it as a top 5 *for audit effort*

[1] For more about the African Union's digital transformation strategy, see https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf
[2] For an example of digital transformation in Ghana from the World Bank, see https://blogs.worldbank.org/africacan/ten-facts-about-digital-technology-adoption-ghana
[3] For more about cyberattacks in Africa, see https://african.business/2023/06/apo-newsfeed/african-nations-feature-prominently-in-global-top-100-for-online-threats

CYBERSECURITY

While organizations are hurriedly strengthening their cyber defenses, the speed at which some businesses have implemented digital operating systems has not been matched by adequate protection.

In addition, lower levels of expertise and training within organizations often means it can be easy for attackers to prevail. "The people involved in hacking are more sophisticated, better financed, and more well-tooled than those of us who are supposed to understand and keep the lid on cybersecurity," said a CAE from Kenya in financial services.

Focus on relevant risks

Organizations are identifying the wide range of risks they face and focusing resources on those that are most likely to impact them. For example, critical infrastructure attacks tend to use denial of service attacks and ransomware tactics to extort money from those organizations – a common tactic for those also attempting to hack financial institutions, a CAE at a South African bank commented.

In addition, hackers often exploit regulatory requirements – such as Europe's General Data Protection Regulation (GDPR) – to set up compliance-related ransomware attacks. "After GDPR, we noticed attacks specifically targeted at holding businesses to ransom with the threat that they would divulge customers' personal information – a tremendous operational and reputational risk," the South African bank CAE added.

Taking a risk-based approach to identifying and mitigating such attacks is critical where organizational resources are scarce. "You must take whatever information is relevant to your organization and fine-tune it to your needs and contexts so that you do not end up investing in a lot of useless tools that will not achieve your desired objectives," a CAE at a mining business in Zimbabwe said. CAEs at the meeting agreed that ensuring the first and second lines had the most advanced technology tools the business could afford was critical.

Resources

Auditing Cybersecurity Operations: Prevention and Detection

A Global Technology Audit Guide (GTAG) focused on cybersecurity published by The IIA in 2022.

The IIA's Three Lines Model

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

Build awareness

Since Africa depends on a patchwork of emerging cybersecurity frameworks, organizations are striving to educate their staff and governments are focused on building awareness among the general population.

Some government initiatives are already having an impact. In 2022, for example, the National Information Technology Development Agency of Nigeria, which oversees cybersecurity and data protection, created rules and guidelines requiring businesses that

CYBERSECURITY

process personal data to be secure in their data collection, processing, and storage. Similar regulations exist in other countries, including Malawi.

"Regulators specifying what you need to do has helped bring focus when it comes to tackling cybersecurity issues," said Thokozile Kuwali, CAE at NICO, a financial services company in Malawi.

Upskilling urgently needed

While CAEs at the roundtable agreed that internal audit had a critical role to play in raising awareness, internal auditors also need to improve their skills rapidly to help organizations identify, monitor, and mitigate cyberattacks. Often internal audit's own tools are not sophisticated enough to assess and monitor fast-moving risks across the business, or they are too fragmented to provide an enterprise-wide view. Auditors' cybersecurity skills tend to lag behind those of the first and second lines, and there are too few specialist IT auditors in most organizations – all themes that emerged from the discussion.

"A lot of people who fall prone to cybersecurity attacks lack awareness, and that is a huge space for internal audit to move into."

Kuwali said that she had invested heavily not only in monitoring systems and business continuity processes to combat cyber risk, but also in staff awareness and internal audit training, despite obstacles. "Training is expensive in this part of Africa [Malawi] and sometimes you cannot get it and have to go to a country such as Kenya," she said. Because the company's level of digitalization is high, she has managed to automate some internal audit training through a specially designed portal, but constraints remain: "The cost is a challenge, as is availability and the fact that the field is fast moving, so there are always new tools you need to learn how to use and implement," she said.

But it is not just the audit team that can lack skills. In Tanzania, for example, boards are now mandated to have a member who is an expert in IT as well as finance. Understanding of the controls implemented across an enterprise can be patchy – a crucial lack internal auditors can help address. "In each audit we do, we share awareness and help spread best practices across the organization," said a CAE in the public sector in Angola.

A team effort

"A lot of people who fall prone to cybersecurity attacks lack awareness, and that is a huge space for internal audit to move into," a senior auditor in the public sector in Zambia said. But while educating people about threats is useful, it is not sufficient on its own, she said. Success requires a team effort that involves a sense of ownership across all levels of an organization. Internal auditors can help staff get involved and take personal responsibility to help manage the risk. "When people are part of the decision making, they know their input is important and are driven to contribute much more," she added.

CYBERSECURITY

How internal audit can help the organization

1. Assess whether the organization has adopted a risk-based approach to identifying and mitigating cyber risk and review how well investments in defensive technologies align with such assessments.
2. Provide management with an objective evaluation of the effectiveness of cybersecurity processes, policies, procedures, governance, and other controls.
3. Build cybersecurity skills within the internal audit function.

FRAUD

Fighting fraud on multiple fronts

Fraud and corruption have been persistent social challenges, but automation, technology, and strong tone at the top can make a difference.

Africa is rapidly transitioning from manual to digital transaction and record keeping. Digitalization has reduced opportunity for some kinds of fraud. "Many organizations are embracing automation to limit the involvement of human judgment and interference," said a CAE in Uganda. For example, digitalization has automated some government processes that had been performed manually, thus reducing the opportunity for workers to take bribes from the public.

However, even with digitalization, controls can be undermined. For example, a CAE in Uganda said that IT fraud controls at his organization were circumvented by one of the managers responsible for implementing them. That required careful, patient investigation to resolve. Internal audit is seen in many organizations as the key investigator in such fraud cases.

Unfortunately, the increased use of mobile money, online transactions, and government digital services has also increased opportunity for online fraud, said CAEs. "These rapid technological changes have created a knowledge gap in organizations in terms of what controls need to be put in place to make their use safe," said a CAE in the public sector in Ghana. "Those with fraudulent intentions exploit those gaps to their advantage." With fraud risk literacy low among portions of the population, many remain vulnerable to digital hacks and scams.

Survey Results – Fraud

4TH – RISK LEVEL
46% ranked it as a top 5 *for risk level*

1ST – AUDIT EFFORT
57% ranked it as a top 5 *for audit effort*

FRAUD

Roundtable attendees said that the mobile-savvy younger generations seem most likely and capable of exploiting loopholes in digital systems.

Procurement fraud

Organizations must stay vigilant against procurement fraud, particularly in the public sector where contractors can artificially inflate prices on government projects. Introducing more rigorous due diligence processes over third-party contracts helps, especially when they are implemented across the organization.

"Based on our past audit findings, we have now changed the setup so that our divisions do not see themselves as separate entities, but as one institution, which has helped us rapidly share information and standardize procurement processes," a CAE in the public sector in Zambia said.

Internal auditors should also use enterprise-wide data analytics to combat fraud, said Ruth Doreen Mutebe, CAE at a Uganda power company and chair of AFIIA.

Analytics can automatically identify exceptions in a wide range of areas – from procurement to human resources onboarding processes – that point up where fraud or corruption may be taking place. "Internal auditors need to enhance their skills in data analytics and allocate budgets to systems that support it," Mutebe said. Internal auditors can quickly follow up on unusual activity and take any remediation actions needed before it turns into a major issue. Several CAEs at the roundtable said they were implementing such predictive analytics in their organizations.

Visible deterrents

Senior management must set the tone from the top to communicate that the organization is serious about tackling fraud, said roundtable participants. That can come from the very top of government, with several leaders in the region, including Zambian President Hakainde Hichilema, making the fight against fraud part of the national agenda.[4] A clear message from the top will help foster collaboration between government agencies to share data and knowledge on fraud and related activities.

Ultimately, fraud detection must include visible punishment of wrongdoers to act as a deterrent, CAEs at the roundtable agreed. "Internal audit departments are often doing continuous follow up on their work to make sure there is action on the issues raised," a CAE based in Kenya said.

> "People do not always understand what fraud is, but if you make them aware, they are more likely to report it when they see it."

[4] For more about Zambia's crackdown on government fraud, see https://www.africanews.com/2022/03/27/zambia-corruption-crackdown-nets-ex-ministers/

FRAUD

Changing organizational culture is also a fundamental weapon in the fight against fraud risk. "People do not always understand what fraud is, but if you make them aware, they are more likely to report it when they see it," said Zelia Njeza, a regional audit manager at a charitable organization and president of IIA–Tanzania. She said awareness training has been very effective in bringing cases to light and in fostering cooperation between the three lines. CAEs at the roundtable said that they had helped their organizations communicate ethical codes across the business and set firm expectations on behavior.

Courage and tact

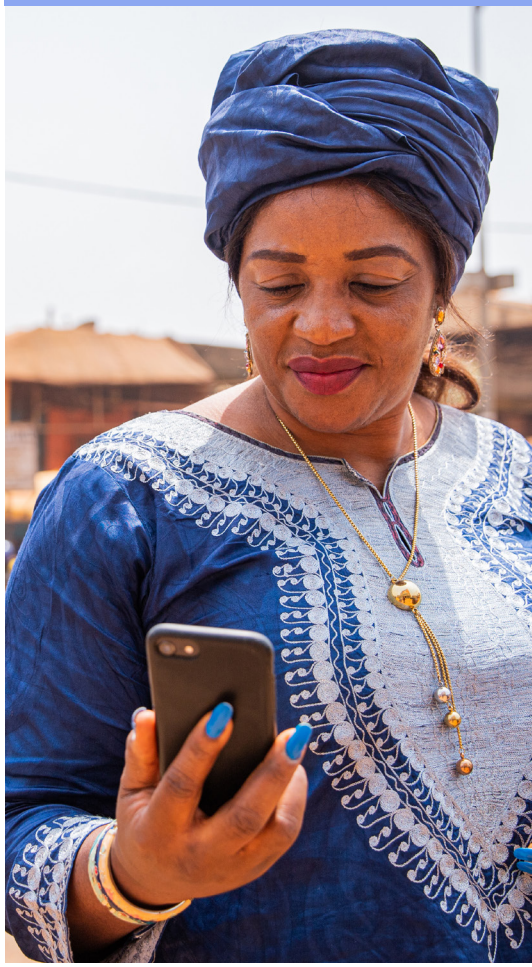
Courage and tact are essential parts of the CAE's tool kit, Mutebe said: "CAEs need to be courageous, but that does not necessarily mean being confrontational. Doing it in a smart way is often more effective."

In some African countries, the internal audit profession is in early developmental stages, which means stakeholders within some organizations may not understand the role of the internal auditor. Executives or senior management who do not really understand the value of internal audit may try to assert influence on CAEs to break down controls. In those circumstances, CAEs must collaborate with the audit committee to educate management about the role of internal audit.

Providing advisory support on strategic initiatives can quickly win management over, said Harriet Karikari, CAE at the Ghana Institute of Journalism and president of IIA–Ghana. To do so, CAEs must be motivated to keep up to date with emerging trends and ensure their skills and competencies are continually refreshed. "CAEs should not limit themselves to financial auditing, but understand they are in the organization to add value across a wide range of areas," she said.

Resource

Internal Audit and Fraud, 2nd Edition (The IIA)



FRAUD

How internal audit can help the organization

1. Assist management with the evaluation of internal controls used to detect or mitigate fraud; evaluate the organization's assessment of fraud risk.
2. Evaluate whether there are opportunities at the organization to reduce fraud through automation.
3. Consider opportunities for using data analytics to identify unusual activity that may be an indicator of wrongdoing.
4. Assess how well ethical codes and the tone at the top are expressed and communicated.
5. Educate management on the importance of fraud prevention controls and the role of internal audit in prevention and detection of fraud.

BUSINESS CONTINUITY

Preparing for new threats

Business continuity took on new priority following the pandemic, and with a growing range of environmental and technology risks on the horizon, CAEs are ensuring that robust business continuity plans are in place.

Since the pandemic, business continuity has moved up the agenda in boardrooms and internal audit functions. While the impact of the pandemic was slower to arrive in parts of Africa than some other regions, when it did, many businesses struggled to survive – and the longer-term effects could make future risks harder to mitigate.[5]

Some countries in the region have seen new threats piled on after the pandemic. "In Malawi, we had COVID-19, cholera, a cyclone, and now we are talking about potentially devaluing the currency," said Thokozile Kuwali, CAE at NICO in Malawi. "Internal auditors need to remain alert, learn from trends, benchmark, and improve readiness to be in a position to counter the effects of whatever comes."

Business continuity plans must be tested, and the resources identified to mitigate risk must exist in real life, rather than only on paper. "[Business continuity planning] is not just a document, it is a living thing. Testing is key because you want to know it will work when the time comes," said Kuwali. A key task is to audit business continuity plans to ensure they cover key risks and to ensure that mitigations are realistic and properly resourced.

Survey Results – Business Continuity

2ND – RISK LEVEL
52% ranked it as a top 5 *for risk level*

2ND – AUDIT EFFORT
56% ranked it as a top 5 *for audit effort*

[5] For more about long-term socio-economic impacts of COVID-19 in Africa from the United Nations Development Programme, see https://www.undp.org/africa/long-term-socio-economic-impacts-covid-19-african-contexts

DIGITAL DISRUPTION AND CLIMATE CHANGE

Dealing with the risks of the future

According to survey responses, CAEs expect digital disruption and climate change to be the fastest growing risk areas in Africa in the next three years. Internal auditors are adapting to these new realities.

Digital disruption opportunities

Slow adoption of technologies can keep business costs high compared with competitors, or cause organizations to miss opportunities as customers jump on the latest tech trend, said Denish Osodo, CAE at Safaricom, a Kenyan telecommunication business. He said that he has pushed his team to use new technologies in their audit work so that they can both improve efficiency and get a firm understanding of how programs work in practice.

"If you can use AI in your own audits, it helps showcase the technology to the business," he said, "and CAEs can expand their offering to advisory work on new technology implementations because management can see you appreciate the risks and opportunities." If internal audit does not have the necessary skills on staff to adopt new technology or AI, co-sourcing with partners and other parts of the business are effective strategies, he added.

Survey Results – Future Expectations

DIGITAL DISRUPTION: Risk rank increased from 8th TO 2nd

CLIMATE CHANGE: Risk rank increased from 13th TO 5th

DIGITAL DISRUPTION AND CLIMATE CHANGE

Visible impacts of climate change

Climate change was the second-fastest climbing risk in the survey after digital disruption. In Africa, floods and cyclones are becoming more common, causing deaths and affecting infrastructure, agriculture, and other sectors.[6] In 2023, for example, Cyclone Freddy wreaked havoc across Southern Africa.[7]

"Climate-related risk has become very real in Africa," said Ruth Doreen Mutebe, CAE at Umeme, a Ugandan power company, and chair of AFIIA. "Boards and management are increasingly asking internal audit to look at climate change, the environment, and sustainability because we are the eyes and ears on the ground."

Mutebe said CAEs needed to educate themselves on the key trends and identify those areas most likely to impact their organizations. That involves reading the literature, training, benchmarking, and understanding the expectations of key stakeholders. She added, "Using data analytics will be helpful, as will doing some predictions for what might be coming next."

"Boards and management are increasingly asking internal audit to look at climate change, the environment, and sustainability because we are the eyes and ears on the ground."

Finally, for reporting requirements that are in place or being added for different countries or industries, internal audit will be heavily involved in ensuring reporting processes are robust, accurate, and timely.

[6] For more about climate impacts in Africa from the World Meteorological Organization (September 2022), see https://public.wmo.int/en/media/press-release/state-of-climate-africa-highlights-water-stress-and-hazards

[7] For more about Cyclone Freddy in Southern Africa, see https://reliefweb.int/report/malawi/southern-africa-snapshot-tropical-cyclone-freddys-impact-february-march-2023

BUSINESS CONTINUITY, DIGITAL DISRUPTION, AND CLIMATE CHANGE

How internal audit can help the organization

1. Evaluate whether business continuity plans are up to date, properly resourced, and tested.
2. Assess the organization's strategic plans and objectives in light of digital disruption and emerging technologies such as AI and blockchain.
3. Stay educated on climate change areas most likely to impact the organization.
4. Assess the organization's readiness for climate-related reporting requirements and ensure appropriate reporting.

ACKNOWLEDGMENTS

Africa Report Development Team

Africa regional liaisons
Ruth Doreen Mutebe –
Chair of the African Federation of Institutes of Internal Auditors (AFIIA) and CAE, Umeme, Uganda
Emmanuel Johannes –
Past Chair of the African Federation of Institutes of Internal Auditors (AFIIA), Founder and President, Kepler Associates, Tanzania

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

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

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.

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