
2024
RISK IN FOCUS
Hot topics for internal auditors
NORTH AMERICA
Read more
Internal Audit FOUNDATION

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.

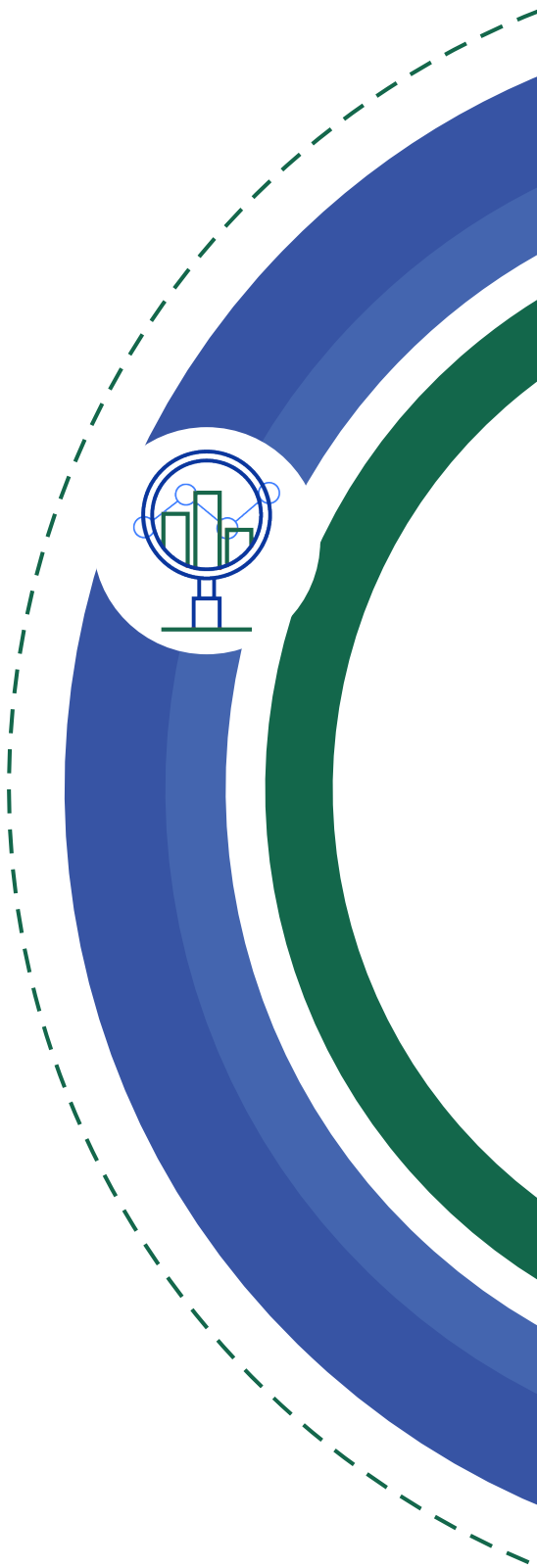
Each of The IIA's six regions will receive two reports:

- **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).



NORTH AMERICA REPORT SPONSOR

AUDITBOARD

CONTENTS

Contents

EXECUTIVE SUMMARY – NORTH AMERICA

Responding to rapid change with collaboration

After an unprecedented three years of global disruption, North American organizations are seeking closer collaboration with stakeholders across their organizations to get in front of the fast-moving risk landscape. Internal audit leaders are often acting as advisors to the board and management on mission-critical projects and retooling audit methodologies to better manage the risks ahead.

North America Risk in Focus provides insight into urgent questions facing CAEs 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?

Two risks dominate the risk landscape for North America in 2024 – cybersecurity and human capital, which cut across almost every aspect of an organization's operations. By 2027, CAEs expect the biggest risk to still be cybersecurity, but digital disruption will leap into second place – with climate change also seeing greatly increased risk levels.

Among survey respondents worldwide, the three areas of highest risk were cybersecurity, human capital, and business continuity. 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.

The North America 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. The featured topics for the North America reports are cybersecurity, human capital, market changes, and business continuity.

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

North America Research Participation

- **442 survey responses** from CAEs and directors
- **Participating countries:** U.S. (385), Canada (57)
- **4 roundtables** with 28 participants
- **9 in-depth interviews**

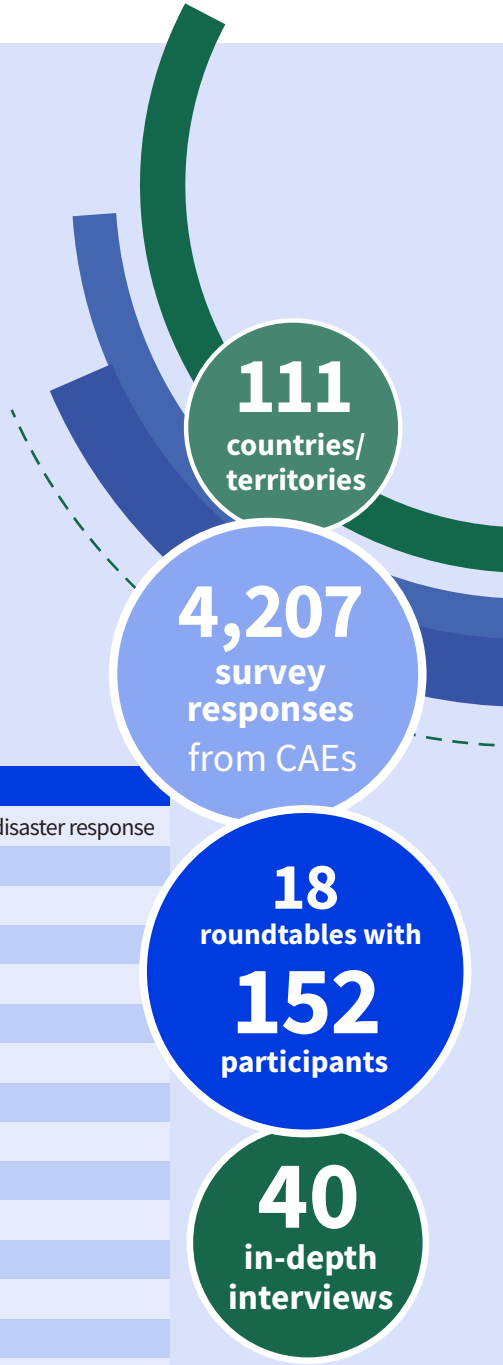
Contents

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 topped 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.

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 from the fourteenth to fifth 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 – NORTH AMERICA

How to use survey results

Key findings for North America are summarized below, 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 – North America

- Cybersecurity and human capital dominated the risk landscape for North America for 2024.
- In the next three years, digital disruption and climate change are the risks expected to increase the most.

Figure 6: Expected risk level change in 3 years – North America

- Digital disruption is expected to move from the sixth highest risk to the second highest in the next three years.
- Climate-related risks climb into ninth position, up from the bottom three.

Figure 7: Current audit effort vs. future audit effort – North America

- Overwhelmingly, CAEs chose cybersecurity as a top 5 area for internal audit effort (84%).
- Second place is held by governance/corporate reporting, but this area is expected to decrease in the future.

Figure 8: Expected audit effort change in 3 years – North America

- Steep rises are expected for activity to deal with digital disruption and climate change.
- Increases are offset by reductions for financial liquidity and governance/corporate reporting.

Figure 9: Current risk levels vs. current audit effort – North America

- Governance/corporate reporting is low risk for organizations (16%) but high effort (55%) for internal audit in North America.
- Effort is low compared to risk for geopolitical uncertainty, market changes, and climate change, but these risks may be addressed through financial liquidity, business continuity, or supply chain.

Figure 10: Future risk levels vs. future audit effort – North America

- Risk levels and effort are expected to be closely aligned in the next three years for the rising risk areas of digital disruption (56% /53%) and climate change (30%/27%).

North America Survey Responses Per Country

United States	385
Canada	57
Total	**442**

SURVEY RESULTS – NORTH AMERICA

Understanding the impact of SOX in North America on survey results

To better understand audit activities in North America, it's important to recognize the effect of Sarbanes-Oxley (SOX) requirements and ERM responsibility on internal audit functions, says Richard Chambers, senior audit advisor at AuditBoard.

The Sarbanes-Oxley Act of 2002 established extensive regulatory requirements for internal controls over financial reporting for publicly traded companies in the United States. Internal audit is often tasked with the lion's share of this effort, with 67% of internal audit functions at publicly traded companies saying they have direct responsibility, according to The IIA's 2023 North American Pulse of Internal Audit survey.[1]

In the Risk in Focus survey, Sarbanes-Oxley activity falls under the category of organizational governance/corporate reporting. This area ranked near the bottom for risk (16% as one of their top 5), but it ranked second for audit time and effort (55% at top 5). This effort toward corporate reporting tends to draw audit time away from other areas, increasing gaps between risk and effort in other areas.

In addition to the bandwidth challenge, Chambers noted that Sarbanes-Oxley can also create an independence challenge for internal audit. Among 2023 Pulse survey respondents, 72% of CAEs at publicly traded companies say they report administratively to the chief financial officer (CFO), who is often in charge of the SOX program.

This high level of responsibility for SOX, combined with administrative reporting to the CFO, creates a risk that CAEs are not only providing assurance for internal controls over financial reporting, but are also taking on the CFO's compliance responsibilities directly. At issue is internal audit having enough independence to provide assurance for internal controls over financial reporting, given its responsibilities and reporting line.

Finally, almost half of CAEs at publicly traded companies (46%) are also responsible for ERM, according to 2023 Pulse survey respondents. On the positive side, when one role is responsible for both, there may be closer alignment between risk assessment and audit activity. However, it's important for CAEs to be properly trained in ERM methodology, which places equal emphasis on opportunities and risk. Finally, if internal audit is responsible for ERM, it is preferable for a third party to provide assurance for the overall effectiveness of risk management because the internal audit function should not audit its own activity.

Recommended Reading

The IIA's Three Lines Model

Risk in Focus frequently refers to the influential Three Lines Model, which explains the roles of the first, second, and third lines.

The IIA's North American Pulse of Internal Audit

This annual report provides benchmarks about budgets, staff, and CAE responsibilities.

[1] For survey results cited from the Pulse of Internal Audit, see page 43 (reporting lines) and page 35 (ERM responsibility) at https://www.theiia.org/en/resources/research-and-reports/pulse/

Figure 5:

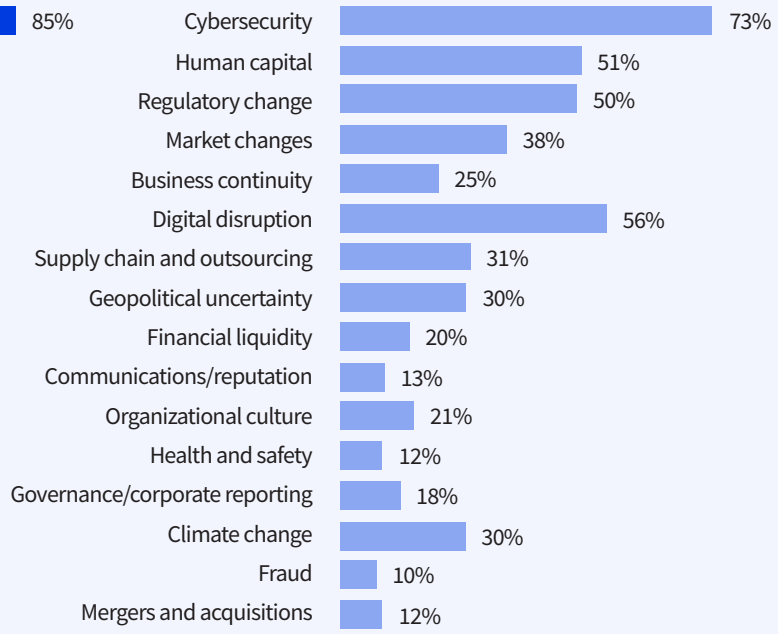
Current risk levels vs. future risk levels – North America

Current risk
Future risk

- Cybersecurity and human capital dominated the risk landscape for North 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, North America, *n* = 442. Percentage who ranked the area as one of their organization's top 5 highest risks.

Figure 6:

Expected risk level change in 3 years – North America

Expected risk change

- Digital disruption is expected to move from the sixth highest risk to the second highest in the next 3 years.
- Climate-related risks climb into ninth position, up from the bottom three.

What are the top 5 risks your organization currently faces?		What are the top 5 risks your organization will face 3 years from now?	
1. Cybersecurity	85%	1. Cybersecurity	73%
2. Human capital	65%	**2. Digital disruption**	**56%**
3. Regulatory change	43%	3. Human capital	51%
4. Market changes	41%	4. Regulatory change	50%
5. Business continuity	36%	5. Market changes	38%
6. Digital disruption	**36%**	6. Business continuity	35%
7. Supply chain and outsourcing	36%	7. Supply chain and outsourcing	31%
8. Geopolitical uncertainty	28%	8. Geopolitical uncertainty	30%
9. Financial liquidity	28%	**9. Climate change**	**30%**
10. Communications/reputation	21%	10. Organizational culture	21%
11. Organizational culture	21%	11. Financial liquidity	20%
12. Health and safety	17%	12. Governance/corporate reporting	18%
13. Governance/corporate reporting	16%	13. Communications/reputation	13%
14. Climate change	**12%**	14. Health and safety	12%
15. Fraud	9%	15. Mergers and acquisitions	12%
16. Mergers and acquisitions	8%	16. Fraud	10%

Note: The IIA's Risk in Focus Global Survey, North America, *n* = 442. Percentage who ranked the area as one of their organization's top 5 highest risks.

Figure 7:

Current audit effort vs. future audit effort – North America

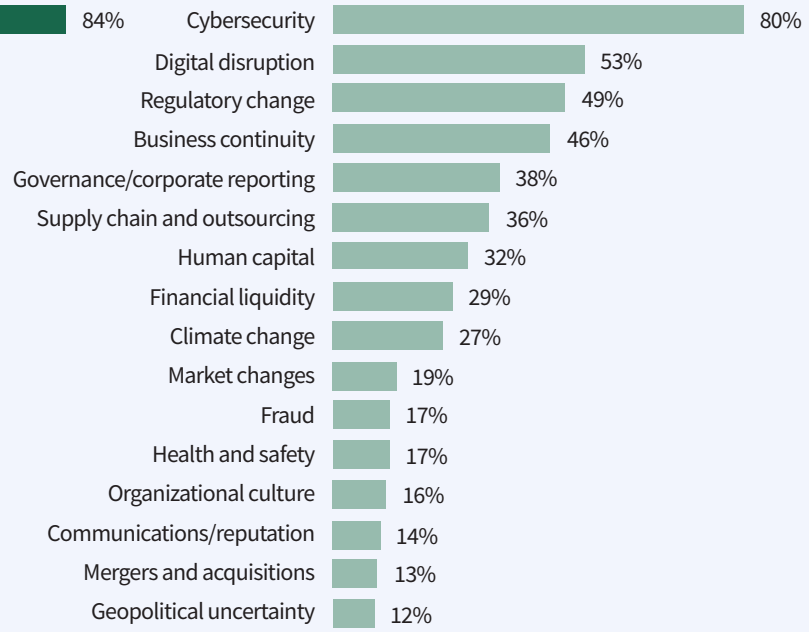
Current effort

Future effort

- Overwhelmingly, CAEs chose cybersecurity as a top 5 area for internal audit effort (84%).
- Second place is held by governance/corporate reporting, but this area is expected to decrease in the future.

What are the top 5 risks on which 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, North America, *n* = 442. 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 – North 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 and governance/corporate reporting.

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

1.	Cybersecurity	84%
2.	Governance/corporate reporting	55%
3.	Business continuity	53%
4.	Regulatory change	53%
5.	Financial liquidity	46%
6.	Supply chain and outsourcing	38%
7.	Fraud	26%
8.	Human capital	26%
9.	**Digital disruption**	**25%**
10.	Health and safety	21%
11.	Communications/reputation	20%
12.	Organizational culture	17%
13.	Market changes	14%
14.	Mergers and acquisitions	10%
15.	**Climate change**	**9%**
16.	Geopolitical uncertainty	4%

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

1.	Cybersecurity	80%
2.	**Digital disruption**	**53%**
3.	Regulatory change	49%
4.	Business continuity	46%
5.	Governance/corporate reporting	38%
6.	Supply chain and outsourcing	36%
7.	Human capital	32%
8.	Financial liquidity	29%
9.	**Climate change**	**27%**
10.	Market changes	19%
11.	Fraud	17%
12.	Health and safety	17%
13.	Organizational culture	16%
14.	Communications/reputation	14%
15.	Mergers and acquisitions	13%
16.	Geopolitical uncertainty	12%

Note: The IIA's Risk in Focus Global Survey, North America, *n* = 442. Percentage who ranked the area as one of their top 5 for audit time and effort.

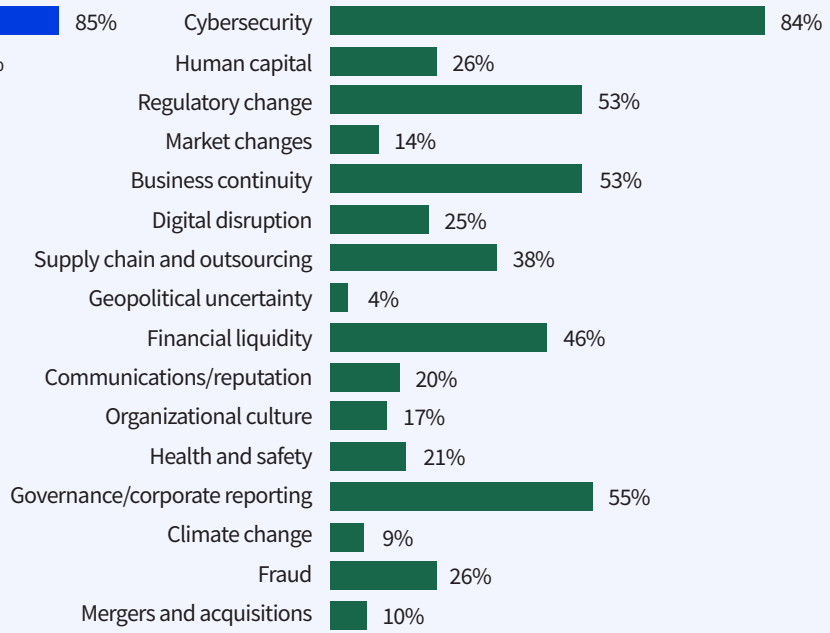
Figure 9:

Current risk levels vs. current audit effort – North America

- Governance/corporate reporting is low for risk (16%) but high for audit effort (55%).
- Effort is lower priority compared to risk for geopolitical uncertainty, market changes, and climate change, but these risks may be addressed through financial liquidity, business continuity, or supply chain.

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, North America, *n* = 442. Percentage who ranked the area as one of their top 5 for risk or internal audit effort.

Figure 10:

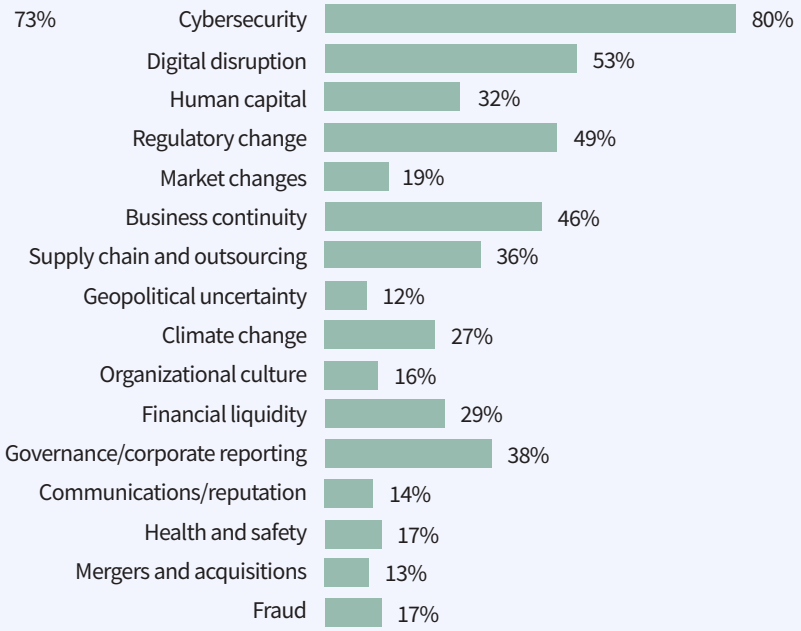
Future risk levels vs. future audit effort – North America

Future risk
Future effort

Risk levels and effort are expected to be closely aligned in the next 3 years for the growing risk areas of digital disruption (56% to 53%) and climate change (30% to 27%).

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, North America, *n* = 442. Percentage who ranked the area as one of their top 5 for risk or internal audit effort.

CYBERSECURITY

Team building for cyber resilience

Because most organizations expect to be hacked, they are focused on building resilience through enterprise-wide collaboration and continuous training.

The pandemic forced many organizations to rapidly roll out IT systems, often using cloud-based third-party suppliers, to enable staff to work from home during lockdowns. As a result, hacking both intensified and industrialized just at the time when extended networks were most vulnerable. Not only has the risk of state-sponsored cyberattacks increased because of geopolitical uncertainty – including the war in Ukraine and tensions between the U.S. and China – but the burgeoning cyber-attack-as-a-service industry means that amateur hackers can carry out sophisticated scams for a fraction of the time and cost.[2]

Those trends have increased both the potential financial impacts of successful breaches and the risk of existential threat from so-called wiper attacks: experts fear that such knock-out hits currently targeting Ukrainian networks could spread to the U.S.[3] The average cost of a data breach in North America has climbed 12.7% since 2020 to $4.35 million in 2022, according to IBM. And 83% of respondents said they had experienced multiple breaches, with 45% of those occurring in the cloud.[4]

Survey Results – Cybersecurity

1ST – RISK LEVEL
85% ranked it as a top 5 *for risk level*

1ST – AUDIT EFFORT
84% ranked it as a top 5 *for audit effort*

[2] For more about cyber-attack-as-a-service, see https://fieldeffect.com/blog/cybercrime-as-a-service
[3] For more about wiper malware, see https://techcrunch.com/2022/02/28/fbi-cisa-ukraine-wiper-malware/
[4] For more about cost of data breaches, see https://www.ibm.com/downloads/cas/3R8N1DZJ

CYBERSECURITY

New SEC rule adds structure

In July 2023, The U.S. Securities and Exchange Commission (SEC) adopted new rules for reporting incidents and disclosing activities related to cybersecurity risk management, strategy, and governance. One of the goals is to make information more consistent and easier to use for decision-makers and investors.[5]

The SEC rules are layered on top of a tangle of existing cyber regulations. There were more than 250 bills or resolutions proposed at state or federal levels in the U.S. in 2021.[6] For those operating across multiple jurisdictions, the time needed to keep up with developments can be significant, said a CAE at a global financial services firm. She described extensive efforts to keep up with requirements, from using cybersecurity consultants to regularly connecting with members of the legal community, the Justice Department, and other CAEs to ensure that the organization is up to speed.

Cyber defense requires knowledge

Awareness of cyberattacks is high in boardrooms and among executive management, but so are talent shortages for key IT and cyber skills, CAEs at the roundtable said. Posts are hard to fill. It's no wonder that human capital ranked as the second biggest risk, with 65% of survey respondents rating it as a top 5 for risk level (see Figure 1). CAEs from small functions and the public sector say understaffing is particularly acute for them because it is hard to compete with the salaries or career prospects from larger companies and the private sector.

Less well-highlighted is the talent gap in the boardroom. Several CAEs at the roundtable agreed that without specialist IT and cyber knowledge on the audit committee or board, recommendations can fall on deaf ears. "Until you get somebody in that oversight position who genuinely understands what needs to be in a program for cybersecurity and data protection, who understands the recommendations from the chief information security officer and internal audit, you are not going to get meaningful progress within the company," said a CAE at a publicly traded North American energy company.

Resources

Assessing Cybersecurity Risk: The Three Lines Model (The IIA)

Auditing Cyber Incident Response and Recovery (The IIA)

Auditing Cybersecurity Operations: Prevention and Detection (The IIA)

[5] For more about the new SEC rules, see https://www.sec.gov/news/press-release/2023-139
[6] For more about cybersecurity legislation in the U.S., see https://www.ncsl.org/technology-and-communication/cybersecurity-legislation-2021

CYBERSECURITY

Some leading organizations elevate the position of chief information security officer (CISO) in the governance structure so that it is easier to pool knowledge, share recommendations, and raise issues. "If the CISO feels there is exposure and the chief information officer refuses to address it, it is critical he or she has the independence to go directly to the CAE or audit committee to be heard," said Karen Percent, a healthcare industry CAE.

Most CAEs at the roundtable said they were strengthening training and awareness to combat continuous developments in malware and social engineering hacks. They get everyone from the CEO down to entry-level staff to participate in ongoing, faux phishing attacks that incorporate recent hacking methodologies, with extra effort where weaknesses have been identified. Setting the tone at the top and making that visible makes a difference.

Organizations are running through extensive hacking, defense, and recovery scenarios to ensure the executive team and board are ready for strategic decision making if a ransomware attack occurs. This is combined with the use of ethical hackers to test online and operational defense controls.

"Building good, trusted partnership is the key to everything we do – being flexible, agile, and listening and collaborating with your business partners is essential."

"You are going to get hacked – it is going to happen," said an academic from a leading U.S. business school, "so the key focus for the board today is to detect and correct."

Collaboration is key to success

Most crucially, collaboration across the entire enterprise is key. Cybersecurity and data security issues are not located in just one part of a business; they are ubiquitous. That means risks, controls, and mitigations also impact multiple business functions. Ada Leung, vice president and CAE at Fidelity in Canada, said that moving to an integrated assurance model[7] has helped her internal audit department identify and focus on higher risk areas. In addition, migrating to an enterprise-wide technology platform meant that the business was able to employ a single risk taxonomy – one language – across its three lines for IT – another plus.

"Just as a business cannot do things in silos successfully, neither can internal audit," she said. "Building good, trusted partnerships is the key to everything we do – being flexible, agile, and listening and collaborating with your business partners is essential."

[7] For more about integrated auditing, see https://www.theiia.org/en/content/guidance/recommended/supplemental/practice-guides/practice-guide-integrated-approaches-to-internal-auditing/

CYBERSECURITY

That also includes listening to staff and watching for potential weak points. Routines that make people's daily jobs difficult, such as clumsy virtual networks, may be circumvented, creating cyber risk control flash points. Management may try to implement solutions outside of IT oversight, creating a "shadow IT" that is ripe for hacking. One solution is to centralize governance processes for cybersecurity in IT departments and away from management so that IT has full visibility into all technology usage.

CAEs at the roundtable said key internal audit assignments have included:

- Collating IT asset management inventories so that patch programs cover the entire enterprise.
- Assessing cybersecurity maturity of the whole enterprise to create a gap analysis of the controls environment.
- Auditing enterprise-wide risk management to test how complete and effective it is for cybersecurity.
- Collaborating with IT and risk management on creating continuous controls monitoring for both cyber defense and operational controls.

In three years' time, survey respondents expect that cybersecurity will still be at the top of the list for risk levels and audit effort. With developing technologies, such as artificial intelligence, coming on stream over that time, and the tensions between the U.S. and China over Taiwan, the risk landscape is only likely to become more complex – and potentially more dangerous.

Management may try to implement solutions outside of IT oversight, creating a "shadow IT" that is ripe for hacking.

CYBERSECURITY

How internal audit can help the organization

1. Assess the level of awareness, knowledge, and skills in key parts of the business, including the board, to ensure that cyber defense responses are relevant and up to date.
2. Evaluate the reporting lines between the CISO, the CIO, and the board to ensure risks and recommendations are communicated clearly and can be escalated to the highest level when necessary.
3. Assess the frequency, timeliness, and effectiveness of faux phishing campaigns and other awareness raising activities and the levels of staff engagement, as well as how well-integrated they are with training and follow-up processes.
4. Use scenario run-throughs to both educate the board on their governance responsibilities and to test that mitigation processes are complete and effective.
5. Evaluate the effectiveness of the controls environment and how well controls are embedded into the first and second lines, paying particular attention to those practices that staff find disruptive or intrusive and are likely to ignore, forget, or circumvent.
6. Evaluate the governance processes around shadow IT and whether it is appropriate for first and second lines to own those technologies and their associated controls.
7. Assess how well the organization's governance structure enables collaboration across the three lines.
8. Assess how well the organization keeps abreast of global developments in cybersecurity and technology regulations reach and how readily data controls can be changed to meet future requirements.

HUMAN CAPITAL

Negotiating the culture clash

At a time of acute skills and talent shortages, CAEs are helping organizations to diversify work practices, recruitment, and retention strategies.

Human capital risk cuts across every strategic and operational area of a business. Without the right people, organizations cannot function effectively – either to achieve goals, or to identify, manage, and mitigate key risks. Because of trends such as digitalization and complex emerging risks such as climate change, organizations require a broader and deeper spectrum of expertise across a wider range of areas. But they face critical shortages in essential skills. In cybersecurity alone, one study put the number of unfilled posts in the U.S. at 750,000.[8]

Accelerated by the pandemic, changes to the culture of work have hit hard in North America. The so-called Great Resignation – a process that saw millions of experienced senior workers quit work as lockdowns triggered a re-evaluation of personal priorities – continues. About 4 million people (2.6% of the U.S. workforce) left their posts in October 2022 alone.[9] In addition, many younger people have fallen out of love with the traditional values and corporate work culture. Not only do most insist on flexible employment practices – including hybrid working – but an increasing number value being part of purpose-driven enterprises.[10]

Survey Results – Human Capital

2ND – RISK LEVEL

65% ranked it as a top 5 *for risk level*

8TH – AUDIT EFFORT

26% ranked it as a top 5 *for audit effort*

[8] For more about cyber staff shortages, see https://www.esentire.com/resources/library/2023-official-cybersecurity-jobs-report

[9] For more about the Great Resignation, see https://www.weforum.org/agenda/2023/01/us-workers-jobs-quit/

[10] For more about hybrid work, see https://www.mckinsey.com/~/media/mckinsey/email/genz/2022/05/17/2022-05-17b.html/ For more about work values, see https://time.com/6176169/what-young-workers-want-in-jobs/

HUMAN CAPITAL

Creating a well-resourced and flexible organizational response is a number-one boardroom priority, CAEs at the roundtable agreed. But that has been made more difficult because of the need to cut costs and fight upward wage demands in an environment that has suffered from inflationary pressures. At the same time, staff are pushing employers to strengthen their diversity, equity, and inclusion (DEI) policies in the workplace. That has seen more firms signing up to voluntarily practice codes proving that they take cultural transformation seriously. In February 2023, more than 100 finance industry organizations across the U.S. and Canada signed up for the industry's voluntary DEI Code.[11]

Middle management sets the tone for hybrid work

But not all senior executives are in tune with hybrid work trends. "Some board members are questioning why we are still hybrid when everybody seems to be returning back to the office," said a CAE in the U.S. public sector. "But hybrid is a key [option] for us because it helps us attract and retain talent."

Adopting hybrid working styles is a popular strategy – but it is not without risk. First, without experiencing real-time, in-person events in the workplace, there are fewer opportunities to develop and coach younger staff, said a CAE at a North American professional services firm. As a result, it takes longer for her hires to absorb the values and culture of the business, especially in more distributed organizations. Second, critical soft skills may be less developed in recently graduated joiners – many of whom completed their college years in front of computer screens as higher education went into lockdown. Interestingly, some of those who experienced online-only higher education want to work onsite. Balancing such conflicting preferences is crucial for attracting and retaining staff, CAEs agreed.

Few companies have fully redefined their work processes in the post-pandemic era. Rather than new cultural expectations being set by the board, culture is more likely to be defined by middle management out of necessity, said Brian Tremblay, CAE at 1stDibs. "Corporate culture is defined by the 'tone in the middle,' where managers make decisions for the benefit of their people, which may or may not align to the organization's values," he said. CAEs can help by providing boards with awareness about differences in work practices across business units so that boards are more in tune with culture realities.

Resources

Talent Management: Recruiting, Developing, Motivating, and Retaining Great Team Members (The IIA)

Cultivating a Healthy Culture (Chartered Institute of Internal Auditors)

2023 Organizational Culture and Ethics Report (AuditBoard)

[11] For more about the finance industry DEI Code, see https://www.cfainstitute.org/en/about/press-releases/2023/dei-code-100-signatories-milestone

HUMAN CAPITAL

Diversity is more than skin deep

A variety of research has shown a positive correlation between increased diversity and economic growth in both the general U.S. economy and in individual businesses.[12] Many organizations have embraced those findings, as has the U.S. federal government, which is implementing new DEI requirements for federal bodies.[13]

Several CAEs at the roundtable said their boards expect their organizations to make extensive use of diversity and inclusion metrics. A CAE at a retail bank said her organization goes beyond tracking physical attributes and also considers diversity in thought, approach, and mindset. Some organizations use the DiSC personality test to better understand the working styles of their employees and maximize employee effectiveness.[14]

Yet while tracking diversity has benefits, caution must be taken to avoid triggering legal action if the statistics demonstrate that some groups have been discriminated against.

Several CAEs at the roundtable said their boards expect their organizations to make extensive use of diversity and inclusion metrics.

Look for non-traditional signs of trouble

Auditing policies, procedures, and the results of employee surveys are obvious internal audit assignments, but they can miss the less obvious signs of trouble. Internal audit can use thoughtful observations to pick up on less-tangible signals – low morale, negative social media, messy breakrooms – and explore whether these are signs of deeper cultural problems.

Collaborate to break down siloed recruitment

A CAE in the education industry echoed a growing sentiment when he said that he had stopped looking at internal audit as a silo within the organization. Instead, he overhauled his department's human resources framework to drop the pretense that internal audit had to be a career for life and ensured that he collaborated with other departments to help improve overall staff retention since all areas of the business are suffering the same challenges.

[12] For more about the positive correlation between diversity and performance, see https://hbr.org/2018/07/the-other-diversity-dividend

[13] For more about the statement on DEI, see https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/25/executive-order-on-diversity-equity-inclusion-and-accessibility-in-the-federal-workforce/

[14] For more about DiSC, see https://www.discprofile.com/products/everything-disc-workplace-profile

HUMAN CAPITAL

Boosting rotations from within the business, increasing the use of guest auditors for specific assignments, and openly discussing new applicants' longer-term career choices helped ease pressure in the internal audit function. "I'm playing the longer game by helping people stay at the business and benefit from an environment of learning, which seems to be working," he said.

Similarly, a CAE at a global analytics company said that his staff often make lateral moves within the organization as a result of having close contact with many business units. Despite the extra effort needed to backfill the internal audit positions, he believes the moves ultimately improve the overall risk maturity of the business.

Capitalize on strengths for internal audit recruiting

While CAEs said they were working to help organizations create the right culture to attract, train, and retain staff within their organizations, many are hampered by staff and skills shortages in their own audit functions – particularly in smaller organizations and the public sector, where budget pressures can be intense.

"I'm playing the longer game by helping people stay at the business and benefit from an environment of learning..."

Although public sector organizations often struggle to offer competitive pay, they can emphasize their public service ethos to increase recruitment and retention, said Pamela Stroebel Powers, The IIA's director of professional guidance for the public sector. "Organizations must set performance expectations up front and make sure people understand how their job relates to the purpose of the organization because every single job in the organization should relate to that mission."

HUMAN CAPITAL

How internal audit can help the organization

1. Evaluate how well management has identified the potential emerging risks of hybrid working and has developed effective strategies and policies to mitigate those risks.
2. Assess the varieties of corporate cultural practices throughout the business and communicate those to the board to feed into decision making and policy setting.
3. Assess the use of formal diversity metrics and their effectiveness in monitoring diversity and inclusion policies, including whether they consider diversity of thought and mind.
4. Develop strategies to use personal interactions with audit clients to identify intangible signs that cultural problems may be brewing and capture those observations for follow up and remediation.
5. Evaluate whether the organization's human resources framework aims to attract and retain talent within the enterprise – rather than within individual silos – and that career progress paths are well-structured and clearly communicated.
6. Assess whether the organization's broader purpose is well-defined and communicated throughout the enterprise, including in human resources strategies for attracting and retaining staff.

MARKET CHANGES

Adding value with strategic involvement

Markets are changing unpredictably, causing organizations to invest in digital strategies that are more responsive to fast-moving trends. CAEs are bringing together expertise across their businesses and acting as advisors on new initiatives to help those transformations.

The economy in North America has driven market changes, competition, and changing consumer behavior over the past year. At the beginning of 2022, the U.S. Federal Reserve turned its attention away from the pandemic to containing inflation, signaling the end of an era of historically cheap money. Business bankruptcies rose as pandemic help faded and customers cut back spending in the face of higher prices.[15] Inflation and a rising dollar made products manufactured in North America more expensive, squeezing domestic margins and pushing imports – especially from China – to pre-pandemic levels.[16] In financial services, some banks collapsed partly because they failed to manage interest rate risk.[17]

At the same time, organizations are adapting to longer-term trends in digital consumerism. Young people have transformed the way consumers interact with organizations – from shopping and service use to activism and public criticism. In a less loyal, more socially connected marketplace, reputations can crash and trigger bank runs in a matter of hours.

Survey Results – Market Changes

4TH – RISK LEVEL

41% ranked it as a top 5 *for risk level*

13TH – AUDIT EFFORT

14% ranked it as a top 5 *for audit effort*

[15] For more about U.S. bankruptcy metrics, see https://tradingeconomics.com/united-states/bankruptcies
[16] For more about global trade, see https://www.globaltrademag.com/increase-in-u-s-container-import-volumes-makes-2023-look-more-like-2019/
[17] For more about bank failures, see https://www.nytimes.com/article/svb-silicon-valley-bank-explainer.html

MARKET CHANGES

Early involvement prevents future problems

Rapidly investing in the technology to deliver products and services is often essential to keep up with the market, CAEs at the roundtable said. But doing so increases exposure to other threats, including cybersecurity for new and untried systems and supply chain risk where services move to the cloud or change their operating structure.

That is why it is critical for CAEs to be involved at the implementation stage as advisors, said Ada Leung, vice president and CAE at Fidelity in Canada. "It is no longer enough to come back three years after a project has been launched and make sure the controls were good. Nowadays, we are collaborating and partnering with the partners to provide assurance of design controls prior to implementation. It is a much safer, cheaper, and more effective approach."

> "Market changes are dynamic risk events in themselves, so CAEs must constantly be alert to re-evaluate what they are auditing and how."

But devising an audit plan for a digitally transforming organization is challenging. "CAEs must be clued into organizational strategies, which means not conducting static risk assessments nor having an event-based audit plan that is inflexible," said Harold Silverman, The IIA's senior director of CAE and corporate governance engagement. "Emerging technologies, market changes are dynamic risk events in themselves so CAEs must constantly be alert to re-evaluate what they are auditing and how." Rather than simply focusing on separate engagements, Silverman said CAEs must update their audit assignments regularly to include those new elements in the audit department's planned work schedule.

That makes sense, first, because risks related to market changes are often embedded in other types of threat, for example, liquidity and financial risk. Second, incorporating market risks into the planned work schedule may enable a CAE to cover that risk without needing to broach it with a reluctant audit committee – even though upward education in risk is an important function of the CAE. Finally, it prevents the internal audit department from neglecting upcoming threats due to an out-of-date audit plan or slow methodologies that do not suit the risk category, he said.

MARKET CHANGES

Calculate the costs of market risks

Organizations need to do more than just identify market risks; they should calculate accurate and specific information about financial impacts, said a CAE at a non-profit healthcare organization. “My goal is to get to ‘What is our unmitigated risk in dollar terms?’ in a way that our executive leadership team can decide which strategic initiatives we are going to pursue or not pursue.”

Ayaka Mitsunari, internal audit director/ risk architect for delivery at Uber, said her team reviews governance processes, strategy, and operating structures to assess whether the business is able to respond effectively to market challenges. For example, internal audit asks, “How is management measuring the stickiness of the product? Do they have the right processes to be able to adapt quickly and innovatively?” she said.

Bring in experts when needed

Given the interconnected nature of the risk and its mitigation strategies, collaborating across the business by tapping into sources of knowledge is key to success. “With accelerated change in markets and customer trends, the future for internal audit and risk management professionals is to be able to partner with senior management on addressing a risk six months from now that you probably have not identified yet. You are going to have to pivot and be flexible,” said a leading academic at the roundtable.

“We do not have [all] the answers in these emerging areas, so we need to be humble, learn, and be attuned to those risk areas where we need to bring in experts if there is a deficiency in the business,” Nancy Russell, CAE at Canada Life. “That could rub against executive egos, but it is important to encourage them to be transparent with the board where solutions do not exist and be open to bringing in help where needed.”

To build business knowledge, CAEs at the roundtable said they strive to hire from a more diverse cohort of staff, especially those with business acumen and experience – although current skills and talent shortages makes that task difficult. To expand internal audit’s range and depth of skills, they also said they focused on boosting certification and training, as well as rotating people through the department and making use of guest auditors on technical issues.

Contents

MARKET CHANGES

How internal audit can help the organization

1. Evaluate the organization's risk management to see if there are adequate horizon-scanning processes to track emerging market trends and use them for strategic decision making.
2. Provide input on market-driven technology projects at the implementation stage to ensure risks are properly assessed and mitigated.
3. Assess how effectively risks from market changes, competition, and consumer behavior are quantified in monetary terms and used in decision-making processes.
4. Assess how well the overall governance processes in the business are responsive to market changes and able to pivot to take advantage of new opportunities.
5. Evaluate the organization's human resources strategies to ensure that key skills and expertise relating to future risks and opportunities are identified – including in the internal audit department – and recruited for in a timely way.

BUSINESS CONTINUITY

Building resilience in complexity

If boards tended to under-prioritize business continuity plans before the pandemic, that is no longer the case. High-profile cyber breaches, extreme weather events, and rising geopolitical tensions – particularly between the U.S. and China – continue to keep the topic on the agenda.

In fact, business continuity, operational resilience, crisis management, and disaster recovery are often not seen as risks in themselves, but as a response to a wide range of potential interruption to the business. "For the systemic risks we face and threats such as supply chain disruption and vendor resiliency, we feel like the answer to all these different things is having a business continuity plan," commented a CAE from a U.S. manufacturer.

Event-based planning is too narrow

The experience of the pandemic and the rapid macroeconomic changes that have driven up inflation and interest rates has not only made it a boardroom imperative to better prepare organizations for the future, but also altered the way businesses think about operational resilience.

Survey Results – Business Continuity

5TH – RISK LEVEL

36% ranked it as a top 5 *for risk level*

3RD – AUDIT EFFORT

53% ranked it as a top 5 *for audit effort*

BUSINESS CONTINUITY

In particular, CAEs at the roundtable agreed that the pandemic mostly overwhelmed those business continuity plans that did exist because of the scale and complexity of the event. Public sector bodies, for example, had to distribute government aid immediately without fraud controls in place. In addition, suppliers, partners, and customers were equally affected so that business continuity plans often failed to account for disruption to those organizations they would normally turn to for support.

"My organization had done a lot of disaster preparedness and planning for local disasters, but this hit everyone all at once, so organizations were not prepared for cross-functional, cross-jurisdictional emergencies of such magnitude," said Pamela Stroebel Powers, director of professional guidance for the public sector at The IIA. Organizations have learned that rapid, unpredictable knock-on risks are a core feature of systemic risks. That means that disasters that are systemic – rather than triggered by a single event, like a storm – fundamentally alter the way that risk can be managed and mitigated during a crisis.

Organizations must plan for both event-based and non-traditional, broad-scope crises. Shannon Urban, vice president and CAE at Hasbro, said her business extended its enterprise risk program to include both types of risk and internal audit ensures they are included, monitored, and that disaster recovery plans are in place. In addition, disaster recovery plans go through regular desktop exercises, where internal audit provides a critical voice so that any weaknesses are proactively identified and tackled.

Detailed risk assessments need deeper collaboration

Given that macroeconomic and geopolitical uncertainty, changes in market behavior, climate change events, and cybersecurity risk share similar characteristics of speed, scale, and complexity, organizations are redrawing the parameters of their disaster response plans and focusing more on organizational resilience. Some CAEs at the roundtable said they felt they were currently in permanent crisis mode, but with limited resources. In some sectors, regulators are pushing for organizations to take a longer-term view of their viability.

Organizations must plan for both event-based and non-traditional, broad-scope crises.

BUSINESS CONTINUITY

"Although the rate of change feels fast now, this is probably the slowest time we will ever operate in as developments such as AI will accelerate faster," said Nancy Russell, CAE at Canada Life. "We need to find out what we and the regulators are comfortable with and what operational resilience means in practice – and because of the dynamics of change in the organization, we have to become comfortable with being uncomfortable as well."

As part of those efforts, organizations must recalibrate risk assessments to creatively connect apparently unrelated or unexpected threats that could combine to interrupt the business. For example, a CAE at a U.S. technology company said 80% of his business's chip-manufacturing capacity was based in Taiwan, which is under potential threat from China. He had been using tabletop scenario-planning to build up an accurate picture of how the company could pivot to meet customer demand in light of possible war, sanctions, or supply chain disruption. "Having continuity plans and resiliency practices in place to either react to or prepare in advance has really helped focus the board about resilience at a strategic level," he said.

Building rich detail into such scenarios is critical because the mitigations that arise as a consequence of dealing with threats can themselves create second and third order risks that need to be mitigated – but that entails collaborating more deeply with management on what can go wrong. "We have made our risk assessment meetings bigger when it comes to crises because it helps management really prepare for longer-term issues," a CAE at a higher education establishment said. Without working together to build such granular, data-driven plans, organizations will flounder when disaster strikes.

"It is more important than ever to meet managers face to face and take the pulse of what keeps them up at night, as well as share what internal audit is monitoring," Hasbro's Urban said. "Nine times out of ten, you do not need a formal audit to drive change – you just need to convince the right people that the problem is really something they should be thinking about."

Resources

Business Continuity Management (The IIA)

Navigating Geopolitical Risk (Chartered Institute of Internal Auditors)

Auditing Third-Party Risk Management (The IIA)

CAEs at the roundtable said they also supported the robustness of risk assessments, governance structures, and relevance of business continuity plans, as well as testing whether the resources are in place to carry out the plan should disaster strike. Many said they implemented a form of combined assurance for their business continuity planning, and some said they co-sourced with external experts and suppliers to make sure they had as few gaps as possible in the range of events covered and in their plans.

BUSINESS CONTINUITY

Planning ahead to fill talent is key

The complexity of such large-scale threats requires operational continuity planning based on high levels of expertise that businesses often do not have in the current human resources crisis – human capital, diversity, and talent management and retention ranked as the second biggest threat in the survey. Key skills and talent are in short supply. Lean business models and automation have stripped out some of the resources needed for such detailed work, said CAEs at the roundtable.

In addition, succession planning for key management posts is an emerging risk. It is common for hard-to-fill, senior vacancies to be open for over a year, especially in areas such as IT and in many other specialties in smaller businesses and public sector organizations. “We are trying to do more and more with less, so we are unable to offer marketable salaries,” a CAE at one university said. “There is no succession plan in place for key roles and it is really impacting business continuity.” If those positions are not filled when an emergency arises, the business continuity plans will not work. Someone must be in place who will take responsibility and has practiced the response plan.

Preparing for regulations on emerging risks that could disrupt the business or its supply chains, such as future U.S.-Chinese sanctions, require organizations to hire expertise in advance. The CAE at the Taiwan connected manufacturing business said that his company was shifting more to software development and needed not only to hire for a strategic change of direction, but also to ensure the company had the regulatory expertise to feed into its business continuity planning exercises.

Most CAEs at the roundtable said they were working to embed business continuity topics in all future internal audits – although the two biggest emerging risk areas – digital disruption and climate change – are both potentially business continuity issues that may demand more attention than expected.

BUSINESS CONTINUITY

How internal audit can help the organization

1. Evaluate how comprehensively the organization's enterprise risk management framework includes both event-based and large-scale disruptive risks.
2. Compare regulatory requirements with the organization's risk appetite to establish a suitable strategy for business continuity planning.
3. Help identify second-order or third-order risks that may arise in complex risk scenarios or because of the negative impact of first-order risk mitigation steps in the business continuity plan.
4. Review business continuity processes to ensure a wide range of voices and expertise contributes to brainstorming and plan creation to foster a longer-term outlook.
5. Support management by providing a critical independent voice at tabletop exercises to evaluate their completeness and to highlight where risk mitigation plans need additional resources or testing.
6. Provide assurance that the resources and personnel identified in disaster recovery and crisis management plans are in place and that the processes and controls that support those plans exist and work during real-time exercises.
7. Evaluate the organization's human capital needs for effective business continuity planning, including the existence of key personnel, expertise in emerging risk areas, and in the internal audit department.

INTERCONNECTED RISKS

Geopolitical uncertainty, supply chain, and regulatory change

Efforts to deal with the widespread impacts of emerging global risks are being hampered by increased regulatory requirements. CAEs are seeking better alignment with risk management in complex areas such as supply chain disruption.

Engage in strategic planning discussions for geopolitical uncertainty

CAEs at the roundtables said that many U.S. Fortune 100 companies had the risk of war on their radar. Influenced by the unexpected invasion of Ukraine by Russia in 2022 and rising tensions with China, organizations have strengthened cybersecurity defenses and revisited risk assessments, mitigations, and scenario testing across a wide range of inter-related threats, they said.

Yet, like many interconnected threats in this report, it would be a mistake to consider macroeconomic and geopolitical risk simply as an individual risk category. If Brazil, Russia, India, China, and South Africa, for example, launched a much-discussed alternative global currency, it could, like other geopolitical decisions, be a key driver for a basket of associated risks that could hit North American businesses unpredictably, fast, and simultaneously across their whole enterprises.[18]

So, while this category ranked low in terms of audit time and effort, those efforts are most likely distributed in activities that may not be on the audit plan, such as stress testing, scenario analysis, and strategic advice.

A CAE from a leading North American global consultancy said: “There is a difference between what is auditable on your audit plan, versus what you’re involved with in the organization, especially when you are in the strategic planning meetings.” He said that CAEs must act as strategic enablers for the board so that they can make informed, rapid decisions in such fast-moving but long-term risk scenarios.

> “There is a difference between what is auditable on your audit plan, versus what you’re involved with in the organization, especially when you are in the strategic planning meetings.”

[18] For more about BRICS currency, see https://foreignpolicy.com/2023/04/24/brics-currency-end-dollar-dominance-united-states-russia-china/

INTERCONNECTED RISKS

Diversify the supply chain before crisis strikes

While the pandemic exposed weaknesses to global supply chain networks as ports closed and trade flow stuttered, North America is still dependent on China for much of its manufacturing. In 2023, China produced 28.4% of global manufacturing output compared with 16.6% for the U.S. – in dollars, $4 trillion and $1.8 trillion, respectively.[19] Recent events have highlighted that too many organizations suffer concentration risk among key suppliers. That may be one reason political rhetoric has switched from decoupling with China to the diversification and resilience of supply chains.[20] The challenge is not simply one of finding a manufacturer in a different location but, more crucially, it is to pivot the whole operational infrastructure to avoid potential logistical and quality issues.[21]

For example, when global toy and games company Hasbro began diversifying away from China several years ago, it needed to invest heavily across its entire operational infrastructure and with third-party partners. "You can't just pick up expertise for manufacturing high-quality products from a country that has been doing it for 50 years and transplant it into a country that has been doing it for 10," said Shannon Urban, vice president and CAE at Hasbro. Partnering to train staff at suppliers and duplicating tooling in multiple locations has both smoothed the process and introduced extra resilience into the business.

> "You can't just pick up expertise for manufacturing high-quality products from a country that has been doing it for 50 years and transplant it into a country that has been doing it for 10."

The initiative at Hasbro sat underneath a broader, management-run transformation program across the whole supply chain infrastructure to strengthen resiliency throughout the business – a major strategic project. Given that automation was a key component of the initiative, internal audit engaged with the project to provide advice on the design of effective controls for those systems and redesigned processes and controls from the outset. This kind of work requires a different skillset from traditional internal audit, so Hasbro has invested in competency assessment, training, and on-the-job coaching for the audit team.

[19] For more about U·S· Statistical Division analysis of manufacturing, see https://worldpopulationreview.com/country-rankings/manufacturing-by-country
[20] For more about the statement on diversifying, see https://www.reuters.com/world/cias-burns-us-needs-de-risk-diversify-away-china-2023-07-01/
[21] For more about the challenges of moving manufacturing, see https://asiatimes.com/2023/06/why-so-much-manufacturing-still-gets-done-in-china/

INTERCONNECTED RISKS

Seek alignment and help on conflicting risks

CAEs at the roundtable agreed that regulation was complicating supply chain restructuring. The rise in expected risk for regulatory change is likely fueled by the proliferation of European-style data protection laws across North America. Unlike in Europe where the General Data Protection Regulation of 2018 is implemented with few changes by countries within the region, North American legislators have taken those concepts and enacted widely different rules from state to state, creating a patchwork of often-conflicting compliance requirements.[22]

"We have reached a situation where providing absolute assurance on data privacy laws is so cost prohibitive that it is basically impossible," said Brian Tremblay, CAE at 1stDibs. He compared the current situation with data privacy to the early days of SOX compliance, where the area was so over-controlled that it soaked up too much internal audit effort.

CAEs at the roundtable agreed that internal audit's time is getting too divided to deal effectively with simultaneous emerging risks and burgeoning compliance. "Just as we are responding to these changes in consumer behavior and investing in technology, the pace of regulatory change at a federal and state level has gone berserk," said a CAE in the healthcare industry. That pressure had made her organization more reactive, she believes, pointing to one reason that internal audit time is often being redirected to regulatory compliance.

Aligning internal audit and risk management is critical, Tremblay said. Like many CAEs of publicly listed companies, he has responsibility for risk management. As part of the role, he helps define risk appetite and privacy policies as well as document how those decisions can provide better clarity on the organization's stance. Collaborating with IT to use enterprise-wide technology solutions to embed privacy controls must be a key strategy if internal auditors are not to be swamped with compliance-related work, he added.

[22] For more about the data privacy laws to be implemented in 2023, see https://secureprivacy.ai/blog/2023-us-consumer-privacy-laws

INTERCONNECTED RISKS

How internal audit can help the organization

1. Support the board in strategic planning to help enable risk-informed decision making on emerging and fast-moving geopolitical and economic risks.
2. Assess the organization's processes to identify, assess, and build mitigation strategies for complex geopolitical risks and encourage them to pay attention to the interconnections between risk categories.
3. Evaluate the organization's supply chain strategy, including whether it has adequately assessed the risks associated with in-country critical infrastructure when relocating regions.
4. Assess the organization's relationship with critical suppliers and evaluate the need for a more collaborative approach around training and capacity building.
5. Evaluate the communication between risk management and internal audit to better align on emerging risks.
6. Assess the maturity of the organization's automated controls systems to help reduce the burden of regulatory compliance.

FUTURE EXPECTATIONS

Pressure grows from digital disruption and climate change

Two areas stood out dramatically for expected increases in risk and audit effort – digital disruption and climate change. CAEs are helping their organizations better understand and manage such and helping to keep a strategic focus.

Rapid developments in artificial intelligence in 2023 were highlighted by the huge media coverage of Open AI's algorithm ChatGPT, a program that creates written documents on request.[23] Roundtable participants said they had been carefully experimenting with the program. "We have been using ChatGPT just to pose questions, get some context, and write papers," a CAE at a retail chain said. "We have even used it for some of the board narratives and write up, but with a lot of caution." None relied on it completely for developing documents, but a CAE at a non-profit healthcare business said it had expedited his research and report writing.

The attraction is obvious – such technologies can improve productivity, competitiveness, and, at a time of higher production costs and a cost-of-living crisis, improve margins. But CAEs at the roundtable agreed users do not always understand potential risks, such as breaching data compliance laws or introducing bias into decision-making processes. Because such technologies are easy to download and use, keeping abreast of those risks is difficult.

Survey Results – Future Expectations

DIGITAL DISRUPTION: Risk rank increased from 9th TO 2nd

CLIMATE CHANGE: Risk rank increased from 15th TO 9th

[23] For more about ChatGPT, see https://www.sciencefocus.com/future-technology/gpt-3/

FUTURE EXPECTATIONS

Audit emerging IT risk at the speed of technology

"The key challenge for internal auditors is to ensure they audit at the speed of technology because disruptive technologies typically do not have the policies, procedures, methodologies, risk assessments, and mitigations that are in place for more established IT," said Harold Silverman, The IIA's senior director of CAE and corporate governance engagement. This requires not only being present with the right knowledge when such projects start within the business, but also hiring the right skills into the audit department.

"Instead of just talking about risk from a negative viewpoint, CAEs should be willing to have a conversation about what the potential advantages are to a greater ESG focus."

Getting a grip on data governance is key. Data governance can be hard to understand in fast-moving businesses, the focus group agreed. That has led some organizations to break down their definitions of governance into more manageable chunks – IP data governance, privacy-related data governance, and so on. Looking across different audits at these smaller topics can help, as can embedding data privacy controls into automated processes.

Climate change risk reporting needs strategic view

Having accurate data and reporting lines will be critical when businesses begin to tackle climate-related risks. Enhanced disclosure is in the pipeline from the SEC, with so-called large, accelerated filers (businesses with $700 million public flotation) having to file on greenhouse gas emissions and other metrics from fiscal year ended 2023.[24] Smaller companies begin filing in 2024. But North American businesses are less active in this area than other regions in the world. With so many pressing high-level risks on corporate agendas, CAEs need to tread carefully in order to educate the board and start conversations that will help them prepare.

"CAEs should be open minded in terms of assessing risks related to ESG topics and talking to executives and their boards about those risks, even from a strategic point of view," says Richard Chambers, senior audit advisor at AuditBoard. "Instead of just talking about risk from a negative viewpoint, CAEs should be willing to have a conversation about what the potential advantages are to a greater ESG focus."

Resources

Auditing Privacy Risks (The IIA)

Harnessing Internal Audit Against Climate Change Risk (Chartered Institute of Internal Auditors)

[24] For more about SEC climate-related rules, see https://www.sec.gov/files/33-11042-fact-sheet.pdf

FUTURE EXPECTATIONS

How internal audit can help the organization

1. Engage with management on emerging technologies to provide risk and controls advice on the implementation of new systems.
2. Evaluate how management structures and thinks about data, including whether the data taxonomy is granular enough to identify and mitigate appropriate risks.
3. Provide assurance that the business identifies core IT systems and processes that can be used to embed privacy and data controls to reduce the compliance burden across the three lines.
4. Evaluate the completeness and accuracy of data processes in the organization that relate to ESG issues, with particular attention to forthcoming regulatory compliance requirements on climate-related disclosures.
5. Proactively broach ESG-related issues – and other emerging risks – with the board, emphasizing the potential upsides of taking a proactive, early-adopter strategic position.

ACKNOWLEDGMENTS

North America Report 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

Roundtable moderator – North America
Harold Silverman –
Senior Director, CAE and Corporate Governance Engagement, The IIA

French translation
IIA–Canada

North America Report Sponsor
AuditBoard

Cover photo
Nova Scotia, Canada, courtesy of Getty Images

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

南京审计大学
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


Future
Focused.
Support our Academic Fund programs, grants & scholarships.
An investment in the Academic Fund is an investment in the future of the profession of internal auditing. Contributions provide professors and students an opportunity to access the resources needed to promote and study internal auditing globally. Generous donors help ensure the future of the profession.
Donate Now. theiia.org/IAFdonate
Internal Audit
FOUNDATION

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