
2024
RISK IN FOCUS
Hot topics for internal auditors
MIDDLE EAST
Read more
Internal Audit FOUNDATION
ARABCIIA
الاتحاد العربي لجمعيات المراجعين الداخليين
Arab Confederation for 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.

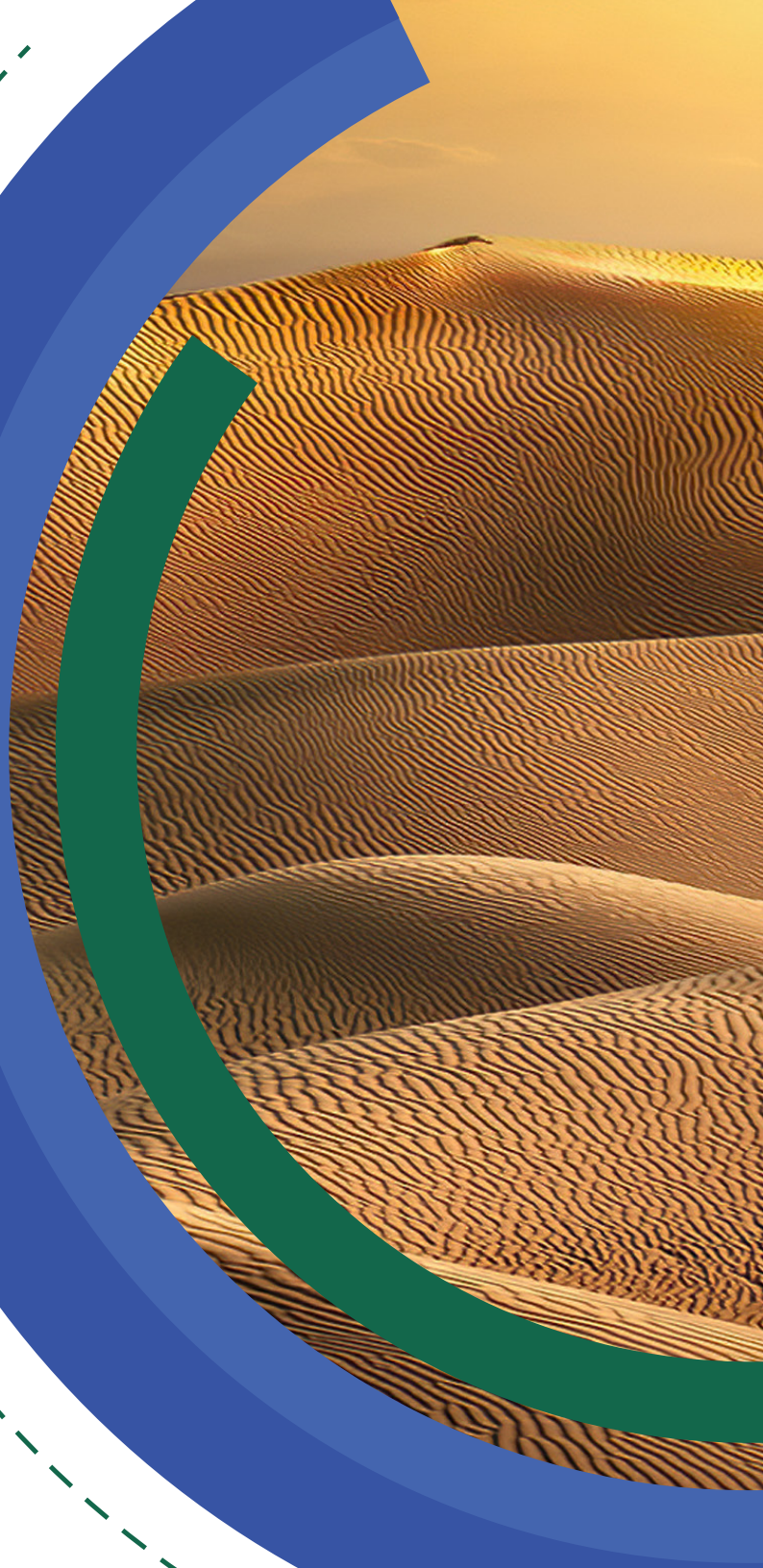
The Risk in Focus methodology was originally created in 2016 by the European Institutes Research Group (EIRG), which continues to publish it in Europe through the European Confederation of Institutes of Internal Auditing (ECIIA).

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).

MIDDLE EAST REPORT SPONSOR

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

CONTENTS



Contents

EXECUTIVE SUMMARY – MIDDLE EAST
Leading the way with professionalism

The Middle East is well-placed to benefit from favorable economic conditions as economies emerge from the pandemic. But in order to thrive, CAEs are supporting organizations to improve professionalism in key areas such as cybersecurity, business continuity, and innovation.

Middle East Risk in Focus 2024 provides insight and audit recommendations 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 the Middle East was aligned with most other regions for having cybersecurity, business continuity, and human capital as top risks, the region was unique in having governance/corporate reporting in its top 5 (see Figure 1).

In the next three years, CAEs in the Middle East expect digital disruption and climate change to be the fastest climbing risks for their organizations, consistent with responses from CAEs worldwide (see Figures 3 and 6).

The Middle East 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 Middle East reports are:

Cybersecurity – Stepping up their levels of internal audit professional competence has helped functions to engage with a wider range of stakeholders and automate audit processes.

Middle East Research Participation

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

Contents

EXECUTIVE SUMMARY – MIDDLE EAST

Business continuity – CAEs are focused on sharpening the scope of their responses and seeking ways to turn crisis into opportunity.

Governance/corporate reporting – The region is investing huge amounts of capital into major infrastructure projects and technology, making good governance a top priority.

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

Contents

METHODOLOGY

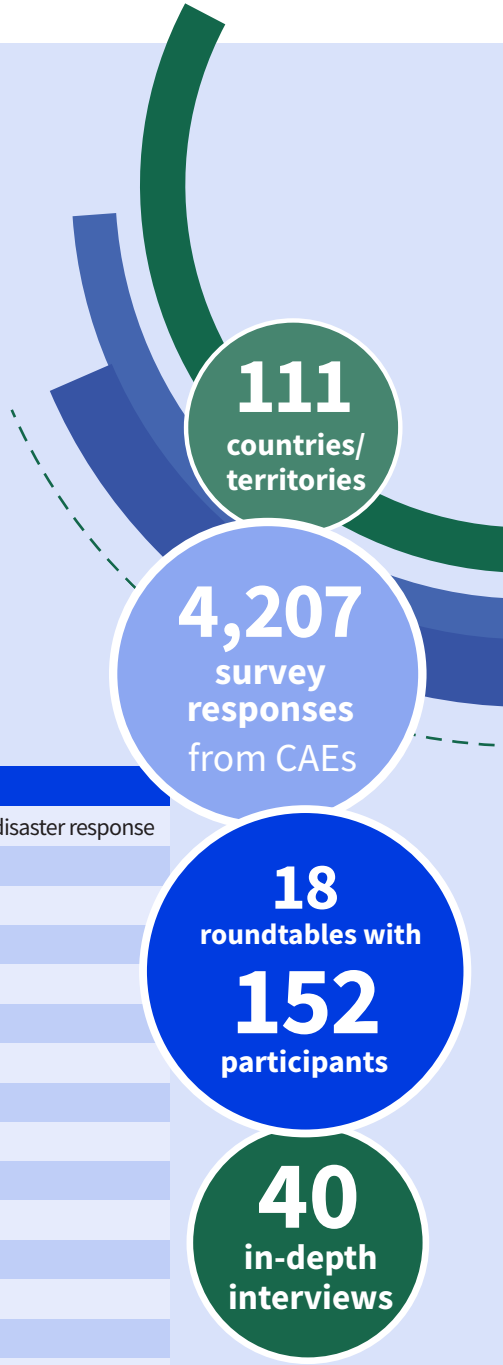
The Risk in Focus methodology starts with a survey of CAEs and heads of internal audit to identify current and emerging risks for each region. The top risks identified in the survey are used in follow-up roundtables and interviews with CAEs, academics, and other industry experts.

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:

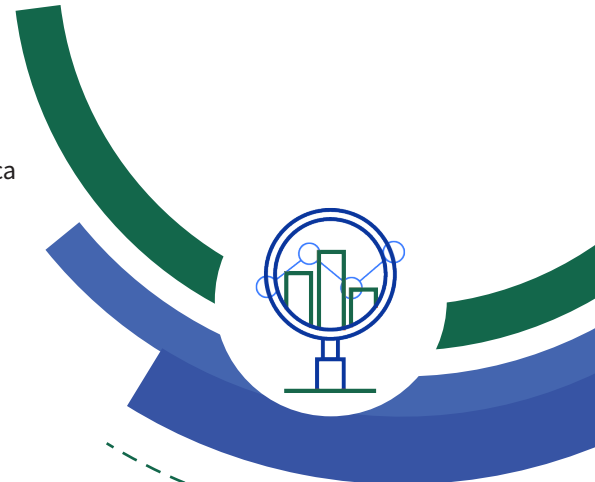
1. Cybersecurity
2. Governance/corporate reporting
3. Business continuity
4. Regulatory change
5. Financial liquidity
6. Fraud

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).



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

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 – MIDDLE EAST

How to use survey results

Key findings for the Middle East 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

- Cybersecurity and business continuity topped the risk rankings in the Middle East for 2024, followed by human capital and governance/corporate reporting.
- In the next three years, risk is expected to ease for business continuity and governance/corporate reporting.

Figure 6: Expected risk change in three years

- Digital disruption is expected to move to second place, with 60% saying it will be a top 5 risk.
- Climate-related risk leaps into sixth position, with 30% saying it will be a top 5 risk.

Figure 7: Current audit effort vs. future audit effort

- Governance/corporate reporting and cybersecurity are the top areas of internal audit effort currently.
- By 2027, digital disruption is expected to replace governance/corporate reporting as a top area of internal audit effort.

Middle East Survey Responses Per Country

Saudi Arabia	89	Algeria	1
United Arab Emirates	29	Bahrain	1
Qatar	18	Iran (Islamic Republic of)	1
Jordan	7	Kuwait	1
Lebanon	7	Palestine (State of)	1
Egypt	5	Turkey	1
Oman	3	Yemen	1
		TOTAL	**165**

SURVEY RESULTS – MIDDLE EAST

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.
- To offset these changes, efforts on governance/corporate reporting, financial liquidity, and fraud are expected to decrease.

Figure 9: Current risk levels vs. current audit effort

- In key areas such as cybersecurity and business continuity, risk and effort are well-matched.
- But there is less alignment in areas such as digital disruption, supply chain, and fraud.

Figure 10: Future risk levels vs. future audit effort

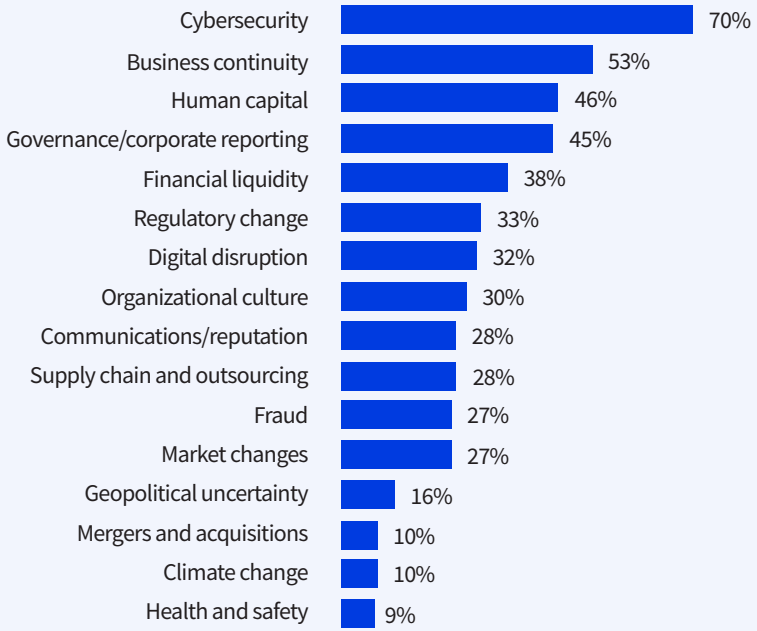
- In the next three years, cybersecurity and digital disruption are expected to share top billing for both risk and audit effort.
- Effort toward governance/ corporate reporting is still expected to outweigh the risk in some organizations.

Figure 5:

Current risk levels vs. future risk levels – Middle East

- Cybersecurity and business continuity topped the risk rankings in the Middle East for 2024, followed by human capital and governance/corporate reporting.
- In the next three years, risk is expected to ease for business continuity and governance/corporate reporting.

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, Middle East, *n* = 165. Percentage who ranked the area as one of their organization's top 5 highest risks.

Figure 6:

Expected risk change in 3 years – Middle East

Expected risk change

- Digital disruption is expected to move to second place, with 60% saying it will be a top 5 risk.
- Climate-related risk leaps into sixth position, with 30% saying it will be a top 5 risk.

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	70%	1. Cybersecurity	60%
2. Business continuity	53%	**2. Digital disruption**	**60%**
3. Human capital	46%	3. Regulatory change	42%
4. Governance/corporate reporting	45%	4. Human capital	38%
5. Financial liquidity	38%	5. Business continuity	37%
6. Regulatory change	33%	**6. Climate change**	**30%**
7. Digital disruption	**32%**	7. Market changes	30%
8. Organizational culture	30%	8. Supply chain and outsourcing	30%
9. Communications/reputation	28%	9. Financial liquidity	29%
10. Supply chain and outsourcing	28%	10. Geopolitical uncertainty	26%
11. Fraud	27%	11. Organizational culture	26%
12. Market changes	27%	12. Governance/corporate reporting	24%
13. Geopolitical uncertainty	16%	13. Fraud	22%
14. Mergers and acquisitions	10%	14. Communications/reputation	18%
15. Climate change	**10%**	15. Mergers and acquisitions	16%
16. Health and safety	9%	16. Health and safety	13%

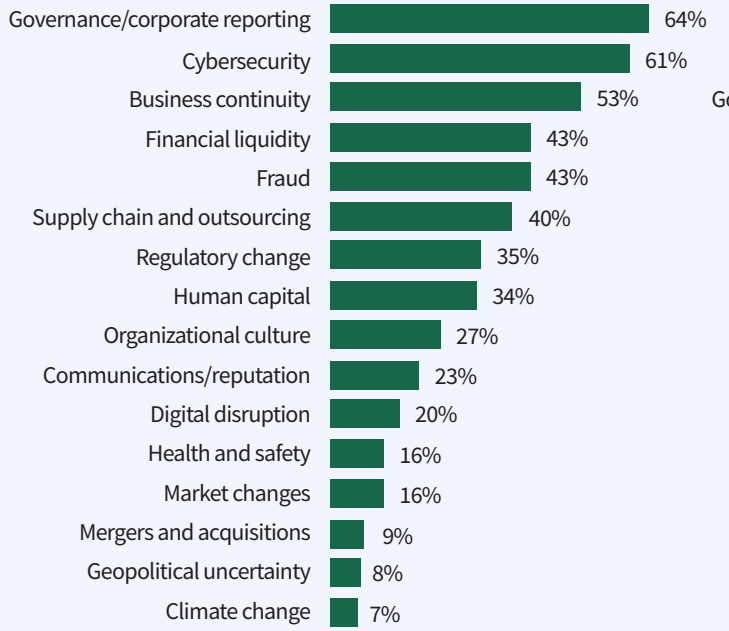
Note: The IIA's Risk in Focus Global Survey, Middle East, *n* = 165. Percentage who ranked the area as one of their organization's top 5 highest risks.

Figure 7:

Current audit effort vs. future audit effort – Middle East

- Governance/corporate reporting and cybersecurity are the top areas of internal audit effort currently.
- By 2027, digital disruption is expected to replace governance/corporate reporting as a top area of internal audit effort.

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?

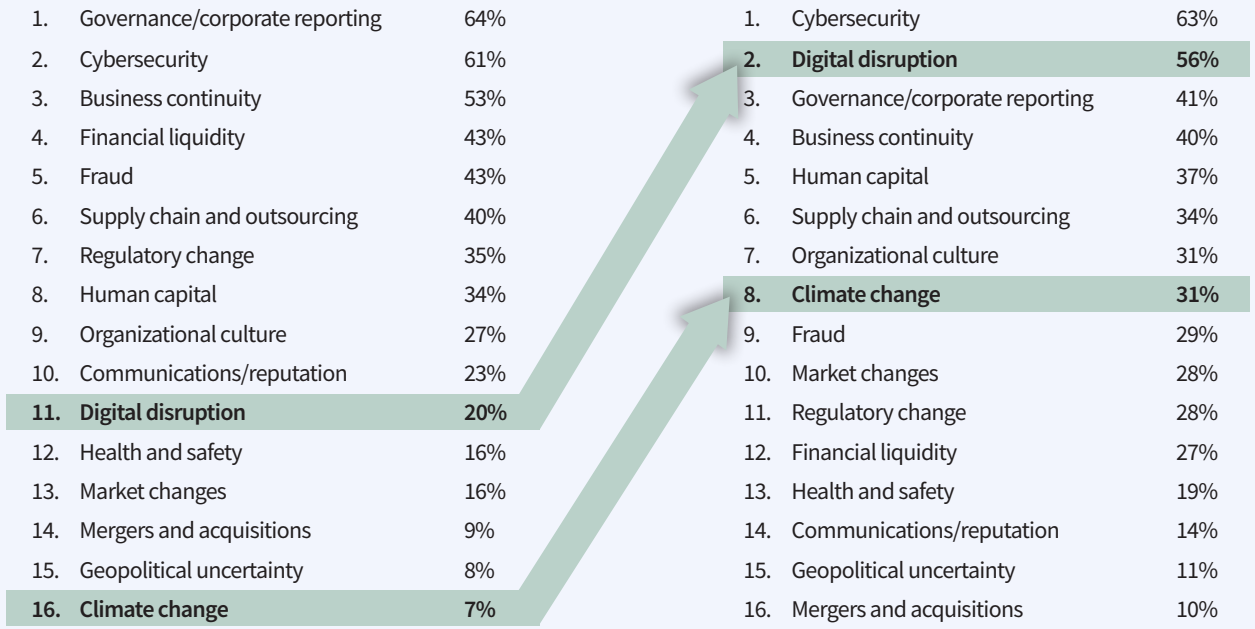
Note: The IIA's Risk in Focus Global Survey, Middle East, *n* = 165. Percentage who ranked the area as one of their top 5 for audit time and effort.

Figure 8:

Expected audit effort change in 3 years – Middle East

Expected effort change

- Steep rises are expected for internal audit activity to deal with digital disruption and climate change.
- To offset these changes, efforts on governance/corporate reporting, financial liquidity, and fraud are expected to decrease.



Note: The IIA's Risk in Focus Global Survey, Middle East, *n* = 165. 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 – Middle East

- In key areas such as cybersecurity and business continuity, risk and effort are well-matched.
- But there is less alignment in areas such as digital disruption, supply chain, and fraud.

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, Middle East, *n* = 165. Percentage who ranked the area as one of their top 5 for risk or internal audit effort.

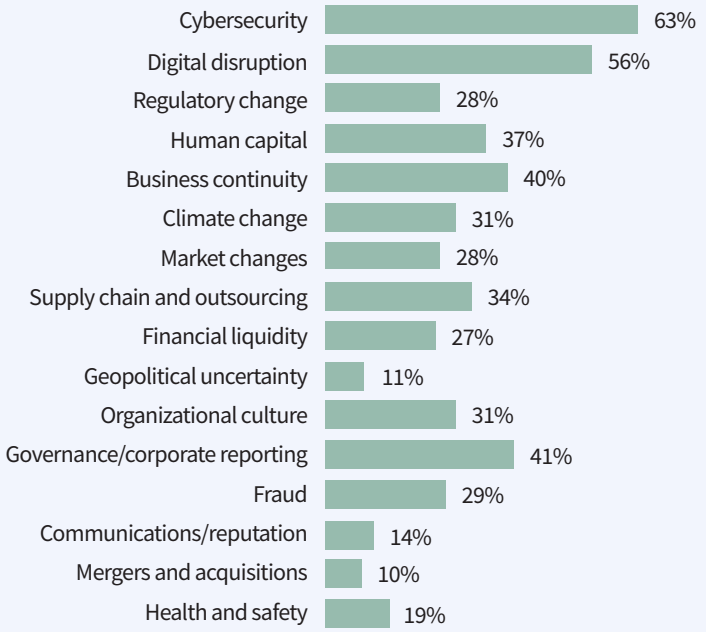
Figure 10:

Future risk levels vs. future audit effort – Middle East

- In the next three years, cybersecurity and digital disruption are expected to share top billing for both risk and audit effort.
- Effort toward governance/corporate reporting is still expected to outweigh the risk in some organizations.

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, Middle East, *n* = 165. Percentage who ranked the area as one of their top 5 for risk or internal audit effort.

CYBERSECURITY

Elevating skills and service

As new technologies are adopted by industries and encouraged by government, cyber risk has increased. CAEs are stepping up their levels of professional competence to engage with a wider range of stakeholders and automate audit processes.

Even prior to the pandemic, the region's digitalization efforts were growing rapidly, with momentum accelerated by COVID-19 lockdowns and efforts to diversify economies away from oil.[1] Middle Eastern countries have become global leaders in digital adoption, as consumers increasingly switch to mobile transactions.[2] But the demand for hybrid work arrangements and third-party collaboration – plus moves to cloud-based infrastructures – have been followed by a spike in cyberattacks.

CAEs at the roundtable agreed that developments in the region to further digitalize would only increase cybersecurity risk. For example, the Kingdom of Saudi Arabia has ambitions to create cutting-edge smart government services,[3] and in the broader region, the financial services industry is fast-transforming into a partnership-led network of highly connected businesses.[4]

Survey Results – Cybersecurity

1ST – RISK LEVEL
70% ranked it as a top 5 *for risk level*

2ND – AUDIT EFFORT
61% ranked it as a top 5 *for audit effort*

[1] For more about how COVID-19 accelerated e-commerce, see https://legatum.mit.edu/wp-content/uploads/2021/03/170321-MIT-Wamda-E-Commerce-COVID19-report-EN-01.pdf
[2] For more about digital consumers in the Middle East, see https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-consumers-in-the-middle-east-rising-adoption-and-opportunity
[3] For more about Saudi Arabia's Smart Government Strategy, see https://www.my.gov.sa/wps/portal/snp/aboutksa/smartstrategy/?lang=en
[4] For more about fintech in the region, see https://www.mckinsey.com/industries/financial-services/our-insights/fintech-in-menap-a-solid-foundation-for-growth

CYBERSECURITY

Regulators boost defenses

"Customer needs are changing, so our risk profile is increasing as they turn towards using fintech over mobile technology," a CAE at a bank in Saudi Arabia said. Since many banks do not have the in-house expertise to implement mobile apps in such a dynamic environment, they are creating alliances with tech-savvy partners. "As banking is moving into more of an ecosystem with open-banking concepts becoming a reality, third-party risk is increasing tremendously," a CAE at a bank in the United Arab Emirates said.

Growing geopolitical uncertainty and related state-backed cyberwarfare is also a concern, although a CAE at a public sector organization in the United Arab Emirates said intergovernmental cooperation against hacker groups was strengthening. One potential weak link, however, was the low maturity of some organizations' business continuity plans, he said.

Some boards in the Middle East still view cybersecurity expenditure as a cost to be avoided, CAEs at the roundtable noted. However, many of the region's regulators have not waited for businesses to act and have introduced regulatory requirements in systemically important sectors. Internal auditors are leveraging these requirements to improve the effectiveness of organizational response to the threat.

> "It is time for us to show management that we are also strategic advisors and are not just there to review policies after the event."

"In terms of cybersecurity support, internal audit is doing well because regulators are requesting that we do specific audit and assurance reviews for cybersecurity," said a CAE at a fintech business.

Strengthening governance

A key area of focus is strengthening governance processes. That includes ensuring that organizations create more detailed policies and procedures, increase the number of staff with certifications, and boost cyber threat awareness across the business.

CAEs are stepping up their levels of professionalism in order to engage with management and the board on advisory assignments. "It is time for us to show management that we are also strategic advisors and are not just there to review policies after the event," said a CAE at a telecommunications business in Oman.

That change of perception is freeing up CAEs to coordinate defenses better across the organization and to help the board not only receive assurance on cyber and data controls, but also to set their strategic objectives on the risk. "We have recently been assessing our cybersecurity risk to make sure that the three-year strategy is in line with the risk appetite of the organization," said a CAE at a bank in the United Arab Emirates.

CYBERSECURITY

Tech skills transform internal audit

Internal audit departments have been investing in cybersecurity skills on staff. CAEs said they had invested in training and professional development programs to boost their internal audit teams' effectiveness. Many also bring in external expertise when needed. When possible, skilled cybersecurity staff are added to the internal audit team.

Abdullah Alanizi, CAE at STC, a telecommunications company in Saudi Arabia, said his board and audit committee supported him in gathering a team of analytics, data, and cyber experts to focus on audit analytics and cybersecurity. They have automated key controls testing, which has increased the effectiveness of the audit function: "We used to audit procurement, for example, every two years," he said. "Now we have translated all of the policies into a program, and we use audit analytics to test it every month."

Another CAE said he had worked with the IT department and senior management to create a live dashboard that showed real-time cybersecurity monitoring metrics. Several CAEs at the group said they had also implemented continuous auditing systems across the business as well as embedded cyber control checks in all audit assignments – with global controls to manage associated risks.

The human factor

"IT teams and internal auditors often focus on technical solutions," said Abdullah Al-Harbi, a partner at HCPA audit firm in Saudi Arabia, "but enhancing cyber risk culture inside organizations is also crucial for mitigating these risks."

He said that internal audit functions played a critical role in helping the business spread awareness of cyber risk throughout their enterprises. "We should enhance our audit universe to ensure we have an overall opinion about the awareness of cyber risk within our companies," said a CAE at a fintech firm said, "because we cannot ensure that awareness is adequate without an effective evaluation of cybersecurity culture within our companies."

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)

CYBERSECURITY

How internal audit can help the organization

1. Evaluate whether third-party organizations have adequate cybersecurity processes and whether the business' operating technology is adequately protected.
2. Assess the organization's governance processes to ensure policies and procedures are sufficiently detailed.
3. Support the board and management as a strategic advisor on cybersecurity, especially in new technology implementations.
4. Implement audit automation and dashboard monitoring in appropriate areas.
5. Assess the maturity of the organization's cybersecurity culture.

BUSINESS CONTINUITY

Preparing proactively before crisis hits

While many businesses were unprepared for the pandemic, the event has propelled business continuity up the board agenda. CAEs are focusing on sharpening the scope of their responses and seeking ways to turn crisis into opportunity.

For many countries in the Middle East, post-COVID recovery has been fast and strong.[5] But CAEs also said that the experience of the pandemic provided much-needed motivation to improve operational resilience and crisis management.

While some CAEs at the roundtable worried that survival had made management overconfident about weathering future disasters, most organizations have been jolted into renewed activity. "Prior to the pandemic, we tended to wait for a catastrophe to happen and react to it," a CAE in the public sector in the United Arab Emirates said. That attitude is quickly changing.

Define scope

"It is important to understand how people define the scope of business continuity," said the director of business continuity and crisis management at a bank in Saudi Arabia. Without a clear scope that identifies the business components and priorities of the plan, it is difficult to define the risk universe or to assign roles and responsibilities and communicate those to internal and external stakeholders. In addition, without a well-communicated purpose, it is all too likely that the process will become a box-ticking exercise where plans are produced and forgotten about, he said.

Survey Results – Business Continuity

2ND – RISK LEVEL
53% ranked it as a top 5 *for risk level*

3RD – AUDIT EFFORT
53% ranked it as a top 5 *for audit effort*

[5] For more on post-COVID recovery in the Middle East from the International Monetary Fund, April 2023, see https://www.imf.org/en/News/Articles/2023/04/13/tr41323-april-2023-mcd-press-briefing

BUSINESS CONTINUITY

The pandemic also demonstrated that most organizations had gaps in their risk universes, CAEs at the roundtable agreed. They said getting it right entails two goals: to capture all of the threats in an increasingly dynamic risk landscape and to develop plans at a deep level of detail to prepare in case the worst happens. "Since the pandemic, we have been changing the mindset within the business so that management thinks about what could go wrong as a kind of general practice in all decisions. That has helped lift the maturity of business continuity in the organization," a CAE at a telecommunications business in Saudi Arabia said.

Business maturity matters

CAEs at the roundtable said that they tailor their business continuity approach to the maturity of the business division in question. Where business continuity is still developing, they support management with advisory assignments to help strengthen risk identification and mitigation strategies. In more mature organizations, they provide assurance to the board that the design and effectiveness of plans are robust. Post-COVID, the level of detail internal auditors assess has increased dramatically – ensuring that second- and third-order risks and mitigations are not only identified but tested by scenario run-throughs.

> "CAEs need to move to real-time monitoring to ensure an agile and speedy response to prevailing risks."

In fact, leading organizations increasingly use business continuity proactively as an aid to strategic decision making. "Internal audit is one of the very few departments in the company that has a holistic knowledge of every single part of the business, which means we can identify areas where the business can capitalize on opportunities," said a CAE from a logistics business in Jordan. During the pandemic, for example, the organization was able to increase revenues by obtaining special transportation permits while other operators had shut down.

CAEs need to move to real-time monitoring to ensure an agile and speedy response to prevailing risks, said a CAE at an investment body in Saudi Arabia. That entails ensuring that business continuity controls are embedded throughout the organization, including in third-party contracts for critical suppliers.

Human capital needs

Talent and competency shortages are hampering business continuity planning in some countries. In fact, human capital challenges ranked as the third highest risk in the region. "Regulations require internal audit to assess the business continuity plan, but I have witnessed many people who do not have the right competencies to do so," a CAE in the public sector in Saudi Arabia said.[6]

CAEs are increasing skills on their teams by investing in professional development from specialist bodies,

[6] For Saudi Arabia's Guidelines for Business Continuity in Government Entities, see https://dga.gov.sa/sites/default/files/2022-10/Guidelines%20for%20Business%20Continuity%20in%20Government%20Entities_0.pdf

BUSINESS CONTINUITY

such as the UK's Business Continuity Institute and others.[7] In addition, internal auditors are collaborating with those who have expertise in ISO 22301 – the business continuity system requirements published by the International Organization for Standardization (ISO).[8]

At the same time, internal audit teams need members with deep business knowledge and experience in business continuity auditing assignments. "It is essential to have a diversified skillset on your audit team in this area," said Tareq Musmali, group chief internal audit officer at Red Sea Global. He recruits from a wide talent pool – from traditional internal auditors to new graduates, engineers, and other specialists, such as data scientists and hospitality subject matter experts.

Musmali also develops diverse skills among those already on staff. "Just as important [as hiring] is the continuous development and upskilling of your staff," he said. That includes working with management to get a deep knowledge of business processes, consistently engaging with the company's risk and resilience team, and attending professionally facilitated training such as workshops and conferences. Musmali also uses collaborative knowledge exchange programs, such as auditor rotations, where auditors spend a period of time in the business and return to internal audit, and guest auditor programs, where employees from the business join internal audit for a specific period and go back into the business with knowledge of internal audit to share. "We try to be independent, but not outsiders," he said.

> "We try to be independent, but not outsiders."

[7] For more about the Business Continuity Institute, see https://www.thebci.org/
[8] For more about ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements, see https://www.iso.org/standard/75106.html

Contents

BUSINESS CONTINUITY

How internal audit can help the organization

1. Assess the scope of the organization's business continuity preparations and whether they are aligned to strategic objectives.
2. Evaluate how well management has developed plans at a deep level of detail to prepare in case the worst happens.
3. Assess the contracts of critical suppliers to ensure they include adequate provisions for business continuity planning.
4. Evaluate whether business continuity plans are designed to take advantage of risk upsides and opportunities.
5. Build diverse skills in the internal audit function through training, hiring, and collaboration.

GOVERNANCE/ CORPORATE REPORTING

Building governance maturity

The region is investing huge amounts of capital into major infrastructure projects and technology. CAEs can play a decisive role in professionalizing governance to support their success.

The Arab Gulf region is currently home to 50% of the world's infrastructure megaprojects – including Neom City, Silk City, King Abdullah Economic City, and Dubailand. Analysts anticipate that before 2030, the region could see its first $1 trillion build.[9]

The speed of deployment means that good governance must be a top priority since policies and procedures around procurement, for example, can make the difference between success and failure. "When a project is executed in fast mode, that can come at a cost in terms of organizational governance," said Maher Al-Aiyadhi, CAE at the Royal Commission for AlUla in Saudi Arabia.

He said that boards should bring in internal auditors to support strong governance from the start of a project. Arriving later in the project can be a risk because the CAE will need to play catch-up. "Management often thinks that at the beginning of a project they do not need an internal auditor because there is nothing to audit," he said. "But that is totally wrong because the auditor can offer advisory services that help build a solid risk culture and ensure projects go in the right direction."

Survey Results – Governance/ Corporate Reporting

4TH – RISK LEVEL
45% ranked it as a top 5 *for risk level*

1ST – AUDIT EFFORT
64% ranked it as a top 5 *for audit effort*

[9] For more about large-scale projects in the Arab Gulf region, see https://www.mepmiddleeast.com/news/gcc-is-home-to-half-the-worlds-megaprojects-reports

GOVERNANCE/ CORPORATE REPORTING

In addition, cultures can quickly become resistant to change. “Management and staff get comfortable and do not want to change their behavior to implement new controls, policies, or procedures,” noted Abdullah Al-Harbi, a partner at HCPA audit firm in Saudi Arabia.

Strengthening corporate culture and reporting to the board can be difficult where internal auditors face budget constraints or lack resources to invest in technology. In some countries, experienced CAEs are in short supply. To help internal auditors to succeed in the region, Al-Harbi said they should adopt a risk-based approach to their work, win the support of the board and audit committee, and keep abreast of emerging risk trends.

Innovation requires caution

Implementing new technologies such as AI is complex and brings with it additional risks the organization should consider, said Abdullah Alanizi, CAE at telecommunications company STC in Saudi Arabia. “We are helping to assess the posture of the organization’s innovation culture,” he said. “It is not the CAE’s job to decide the balance between innovation and risk – but we can assess whether innovation efforts are well-aligned to achieve strategic objectives.”

He says internal audit functions need to take a strategic, proactive, flexible, and collaborative approach on disruptive technologies. Last year, for example, he persuaded his audit committee to allow internal audit to lead a project to coordinate a combined assurance team to help with evaluating emerging technologies. “Internal audit, compliance, risk management, and other internal and external assurance providers work together to share one view, one language, one taxonomy, the same methodology, and a desire to be innovative,” he said.

Using the principles developed through the combined assurance team, Alanizi said internal audit has been cautiously testing AI for use in day-to-day operations, for example, summarizing lengthy documents or looking for overlaps in information.

“It is not the CAE’s job to decide the balance between innovation and risk – but we can assess whether innovation efforts are well-aligned to achieve strategic objectives.”

GOVERNANCE/ CORPORATE REPORTING

Going forward three years, survey respondents from the Middle East said they expect to spend significantly less time on governance/corporate reporting – only 41% said it would be a top 5 area of focus by then, compared to 64% currently. Al-Harbi believes that strategic use of technology is driving this expectation. “Increased use of AI and embedded auditing technologies will help governance issues to be automatically checked and complied with, which will significantly reduce the amount of effort CAEs need to spend on this area,” he said.

Climate change perspectives

Finally, although reporting on climate change or sustainability is not required in many areas, the issues are still being recognized in the Middle East, albeit from a different perspective than typically in the West. A CAE from an investment firm noted, “Western companies appear to be more focused on the reduction of carbon emissions, regulations, compliance, and reporting disclosures. Businesses in the Middle East, on the other hand, are much more interested in looking into what investment opportunities exist, for example, in renewable energy, and what we can do to change and diversify.”

Without significant regulation, internal audit’s time spent on climate change is naturally low, but still important. “CAEs need to make sure that discussions on such strategic issues are taking place at the top level in the organization and that changes in the strategy, or dynamic risk planning, are being carried out effectively once decisions have been made,” he said.

GOVERNANCE/ CORPORATE REPORTING

How internal audit can help the organization

1. Establish a solid risk culture at the outset of major projects, with clearly established controls, policies, and procedures.
2. Assess how well innovation efforts are aligned to achieving strategic objectives.
3. Coordinate with functions across the organization to promote combined assurance with shared taxonomy and methodology.
4. Consider ways to use technology innovation to increase efficiency and productivity for internal audit.
5. Ensure that climate change risks and opportunities are considered in strategic discussions.

ACKNOWLEDGMENTS

Middle East Report Development Team

ARABCIIA
Abdullah Alshebeili –
Secretary General, ARABCIIA (Arab Confederation of Institutes of Internal Auditors); CEO, IIA–Saudi Arabia

Middle East regional liaison
Deema Saud Al Hussain –
Business Development Manager, ARABCIIA

IIA 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