2024 RISK IN FOCUS

Hot topics for internal auditors

ASIA PACIFIC

Read more

Internal Audit FOUNDATION

Asian Confederation of Institutes of Internal Auditors

ABOUT RISK IN FOCUS

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

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

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

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

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

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

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

ASIA PACIFIC REPORT SPONSORS

Asian Confederation of Institutes of Internal Auditors

IIA–Australia
IIA–Hong Kong
IIA–Indonesia
IIA–Japan
IIA–Malaysia
IIA–Philippines
IIA–Singapore

CONTENTS

Contents

EXECUTIVE SUMMARY – ASIA PACIFIC

Navigating political and economic interconnections

Organizations in Asia Pacific have been hit with global headwinds over the past three years, with risks and mitigations uniquely complicated by the high level of economic and political interconnections between countries in the region.

Asia Pacific Risk in Focus 2024 provides insight into urgent questions for organizations and their boards, including:

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

Cybersecurity, business continuity, and human capital are the highest risk areas in Asia Pacific for 2024. These are also the three highest risks globally (see Figures 1 and 5). Over the next three years, CAEs expect climate change and digital disruption to be the fastest climbing risks. This trend is expected in all regions worldwide (see Figure 2).

The featured topics for the Asia Pacific reports are:

Cybersecurity – Organizations are fighting back against cyberattacks through collaboration across the business and utilizing external expertise. Internal audit must focus on evaluating the organization's cyber resilience framework, covering not only prevention and detection, but also monitoring, response, and recovery processes.

Asia Pacific Research Participation

- **1,034 survey responses** from CAEs and directors
- **23 participating countries/territories**
- **3 roundtables** with 26 participants
- **5 in-depth interviews**

Contents

EXECUTIVE SUMMARY – ASIA PACIFIC

Business continuity – In the past business continuity plans gathered dust on the top shelf. Now organizations are using them to help with strategic decision-making and boost organizational resilience. Internal audit must take an updated approach to evaluate business continuity including consideration of its interconnectivity with cybersecurity and operational resilience.

Human capital – When workers move to higher paid opportunities in neighboring countries, organizations are automating processes, realigning human resources strategies, and getting creative. Internal audit is not immune from these challenges and must take them into account when assessing the organisation's human resources processes, as well as for its own resources model.

Regulatory change – With increasingly strict data protection laws and new ESG (environmental, social, and governance) disclosure requirements, internal audit must take a strategic approach to assessing the compliance mechanism, including the organization's ability to respond to rapid changes in the regulatory landscape.

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

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

Contents

METHODOLOGY

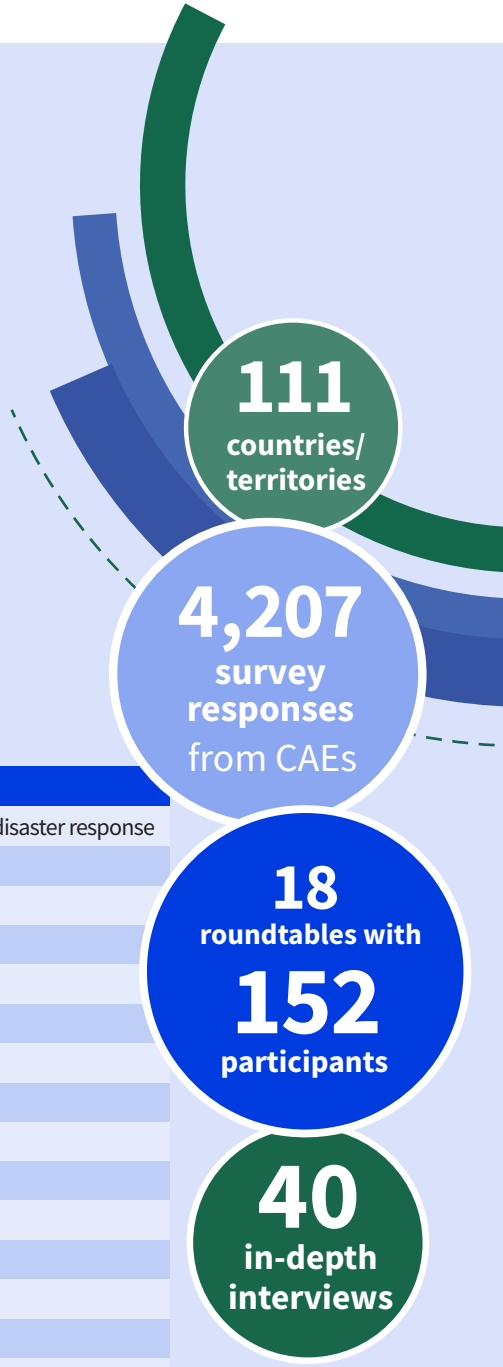
The Risk in Focus methodology starts with a survey of CAEs and heads of internal audit to identify current and emerging risks for each region. The top risks identified in the survey are used in follow-up roundtables and interviews with CAEs, academics, and other industry experts.

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 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 changes (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:

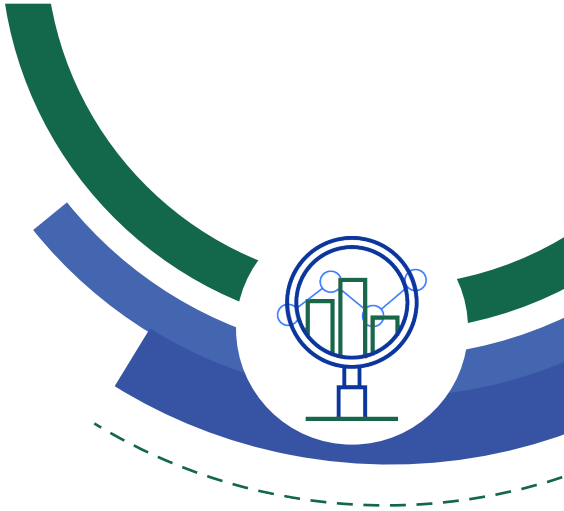
1. Cybersecurity
2. Governance/corporate reporting
3. Business continuity
4. Regulatory change
5. Financial liquidity
6. Fraud

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.

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

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

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

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

Figure 3:

Expected risk change in 3 years – Global

Expected risk change

- Digital disruption is expected to increase from 34% to 55% for those who see it as a top 5 risk.
- 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 – ASIA PACIFIC

How to use survey results

Key findings for Asia Pacific are summarized below, but readers are encouraged to review the graph that follows in detail to obtain further insights. Percentages show how many chose an audit area as one of the five highest for risk level at their organization. Current risk levels are darker blue and future levels are lighter blue. Please note that survey responses primarily came from Japan, Taiwan, and the Philippines, but 20 other countries/territories were also represented.

Figure 5: Current risk levels vs. future risk levels

- Three areas share the highest risk level for Asia Pacific: cybersecurity, business continuity, and human capital.
- In the next 3 years, digital disruption and climate change are the risks expected to increase the most.

Figure 6: Expected risk change in three years

- Digital disruption is expected to move to second place, with 55% saying it will be a top 5 risk.
- Climate-related risks leap into fifth position, with 46% saying it will be a top 5 risk.

Figure 7: Current audit effort vs. future audit effort

- Asia Pacific CAEs were most likely to choose cybersecurity as one of their top 5 areas for internal audit effort (66%).
- Second place was held by a wide variety of areas, including business continuity, regulatory change, and governance/corporate reporting.

Asia Pacific Survey Responses Per Country/Territory

Japan	329	Bangladesh	10
Taiwan	230	Fiji	8
Philippines	103	India	6
Australia	70	Thailand	5
Indonesia	58	Pakistan	4
Singapore	50	Cambodia	3
Malaysia	43	Bhutan	1
Hong Kong	40	Macau	1
Vietnam	27	Maldives	1
China	14	Myanmar	1
Sri Lanka	14	New Zealand	1
Kazakhstan	12	**TOTAL**	**1,031**

Contents

SURVEY RESULTS – ASIA PACIFIC

Figure 8: Expected audit effort change in three years

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

Figure 9: Current risk levels vs. current audit effort

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

Figure 10: Future risk levels vs. future audit effort

- In three years, CAEs expect the gap between key risks and internal audit effort to be more narrow in most areas.
- Cybersecurity is expected to continue at top billing for both risk and audit effort, with digital disruption and business continuity nearby.

Figure 5:

Current risk levels vs. future risk levels – Asia Pacific

Current risk
Future risk

- Three areas share the high risk level for Asia Pacific: cybersecurity, business continuity, and human capital.
- In the next three 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, Asia Pacific, *n* = 1,034. Percentage who ranked the area as one of their organization's top 5 highest risks.

Figure 6:

Expected risk change in 3 years – Asia Pacific

Expected risk change

- Digital disruption is expected to move to second place, with 55% saying it will be a top 5 risk.
- Climate-related risk leaps into fifth position, with 46% saying it will be a top 5 risk.

What are the top 5 risks your organization currently faces?

1.	Cybersecurity	66%
2.	Business continuity	61%
3.	Human capital	59%
4.	Market changes	47%
5.	Regulatory change	35%
6.	**Digital disruption**	**30%**
7.	Geopolitical uncertainty	28%
8.	Supply chain and outsourcing	27%
9.	Governance/corporate reporting	24%
10.	Organizational culture	23%
11.	**Climate change**	**22%**
12.	Fraud	22%
13.	Financial liquidity	21%
14.	Communications/reputation	18%
15.	Health and safety	12%
16.	Mergers and acquisitions	4%

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

1.	Cybersecurity	64%
2.	**Digital disruption**	**55%**
3.	Business continuity	51%
4.	Human capital	50%
5.	**Climate change**	**46%**
6.	Market changes	42%
7.	Geopolitical uncertainty	38%
8.	Regulatory change	31%
9.	Supply chain and outsourcing	26%
10.	Governance/corporate reporting	17%
11.	Financial liquidity	17%
12.	Organizational culture	16%
13.	Communications/reputation	15%
14.	Fraud	15%
15.	Health and safety	10%
16.	Mergers and acquisitions	9%

Note: The IIA's Risk in Focus Global Survey, Asia Pacific, *n* = 1,034. Percentage who ranked the area as one of their organization's top 5 highest risks.

Figure 7:

Current audit effort vs. future audit effort – Asia Pacific

- Asia Pacific CAEs were most likely to choose cybersecurity as one of their top 5 areas for internal audit effort (66%).
- Second place was held by a wide variety of areas, including business continuity, regulatory change, and governance/corporate reporting.

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, Asia Pacific, *n* = 1,034. 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 – Asia Pacific

Expected effort change

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

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

1.	Cybersecurity	66%
2.	Business continuity	59%
3.	Regulatory change	56%
4.	Governance/corporate reporting	54%
5.	Fraud	42%
6.	Financial liquidity	35%
7.	Human capital	33%
8.	Supply chain and outsourcing	33%
9.	Market changes	23%
10.	Organizational culture	23%
11.	Communications/reputation	21%
12.	**Digital disruption**	**19%**
13.	Health and safety	18%
14.	**Climate change**	**10%**
15.	Geopolitical uncertainty	6%
16.	Mergers and acquisitions	3%

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

1.	Cybersecurity	69%
2.	Business continuity	55%
3.	**Digital disruption**	**49%**
4.	Human capital	39%
5.	Regulatory change	39%
6.	**Climate change**	**37%**
7.	Governance/corporate reporting	36%
8.	Market changes	28%
9.	Supply chain and outsourcing	28%
10.	Fraud	26%
11.	Organizational culture	20%
12.	Financial liquidity	20%
13.	Geopolitical uncertainty	18%
14.	Communications/reputation	16%
15.	Health and safety	12%
16.	Mergers and acquisitions	7%

Note: The IIA's Risk in Focus Global Survey, Asia Pacific, n = 1,034. 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 – Asia Pacific

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

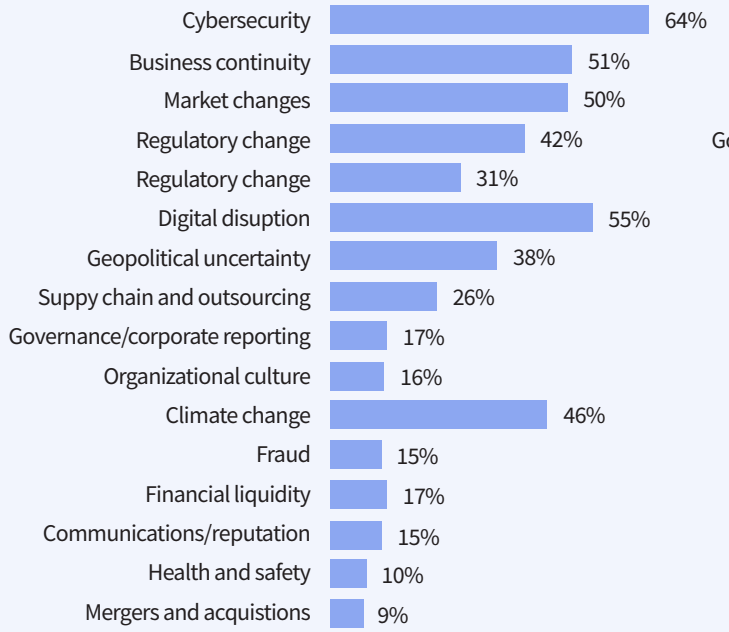
Note: The IIA's Risk in Focus Global Survey, Asia Pacific, *n* = 1,034. Percentage who ranked the area as one of their top 5 for risk or internal audit effort.

Figure 10:

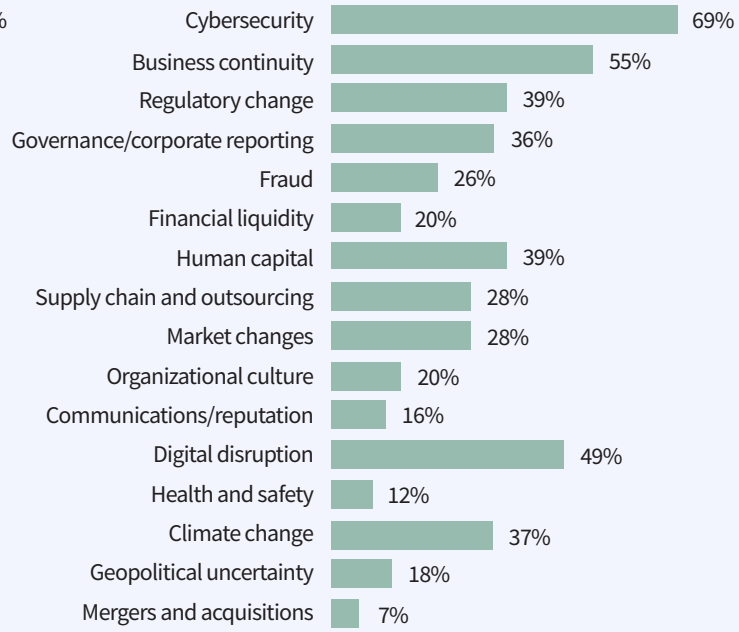
Future risk levels vs. future audit effort – Asia Pacific

- In three years, CAEs expect the gap between key risks and internal audit effort to be more narrow in most areas.
- Cybersecurity is expected to continue at top billing for both risk and audit effort, with digital disruption and business continuity nearby.

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, Asia Pacific, *n* = 1,034. Percentage who ranked the area as one of their top 5 for risk or internal audit effort.

CYBERSECURITY

Facing the onslaught of cyberattacks

Organizations are fighting back against cyberattacks through collaboration across the business and building cyber resilience. In 2022, organizations in the Asia Pacific region experienced more cyberattacks than any other global region, according to one annual survey.[1]

One case in point, a CAE from South Korea estimated that attacks against the country's public sector had quadrupled over the past two years. In addition, he said, attacks were faster, smarter, and often employed advanced methodologies, sometimes selecting specific staff members to target with sophisticated social engineering techniques.

Well-organized and resourced criminal gangs – often supported by armies of amateurs using software-as-a-service hacking tools – have industrialized attacks. Not only that, but threats from nation-sponsored hackers is growing. At the same time, many organizations are pivoting to cyber resilience, including monitoring, response, and recovery – recovering quickly and bouncing back better rather than averting an attack.

Ransomware attacks are another persistent threat. "Cybercriminals and global-state actors are at the forefront in targeting critical infrastructure, sensitive business information, and data, including intellectual property. Consequently, a major cybersecurity breach can result in

Survey Results – Cybersecurity

1ST – RISK LEVEL
66% ranked it as a top 5 *for risk level*

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

[1] For more about cyberattacks in Asia Pacific, see https://www.ibm.com/downloads/cas/DB4GL8YM, page 7.

CYBERSECURITY

material financial losses, reputational damage, and operational disruption if not properly mitigated," said Melanie Tolentino Oteyza, Group CAE of Meralco in the Philippines. "There is a need to strengthen advance security monitoring and fortify cybersecurity measures."

The level of investment needed in cybersecurity defenses is escalating and fast becoming a risk in itself. "It is basically eating into the capital requirements of our financial services arm and imposing another risk," said a CAE in Malaysian financial services firm.

Switch to cyber resilience

CAEs at the roundtable acknowledge that hackers regularly break into organizations' networks, even if defenses are well-implemented. "It is the first time that we have had an extreme risk on our risk register that has been accepted by our oversight board," said an assurance manager in higher education in Australia. "They now realize that despite everything we do, we still won't be able to stop all attacks."

The new approach is to minimize impact and prevent access to key systems and information. To that end, perimeter defenses remain important, but organizations are increasingly identifying mission-critical systems and data and layering them with extra protection.

At the same time, many organizations are pivoting to cyber resilience – surviving rather than averting an attack. This strengthens the essential link between cybersecurity and business continuity. "The same activities that manage cyber resilience well are likely to be the same activities that manage business continuity and resilience," said Adam Stock, partner at PwC in Australia, "so it is imperative CAEs do not look at these risks in silos."

Collaborate across functions

Given the velocity and intensity of the threat, roundtable participants said it was imperative that the first line has well-funded technological defenses, a strong control environment, real-time monitoring, and rapid remediation procedures that are regularly tested. CAEs must have visibility over these processes and, ideally, have the skills and technical know-how to provide a real-time assessment of the impact of breaches and incidents as they occur. This requires internal audit to collaborate broadly across the organization.

"To tackle cyber threat, CAEs really need to collaborate with other assurance or control functions," said Helen Li, CAE of The Bank of East Asia.

For example, she said IT, risk management, and compliance generally manage defenses from an internal perspective, while external experts monitor security operations round-the-clock, and conduct penetration tests and simulated hacking attempts on a periodic basis. Many of these activities are hyper-specialized and focus on technical issues, but internal audit can take a more holistic view and spot gaps and duplications. "We can offer a fresh pair of eyes and critically challenge the status quo," Li said.

CYBERSECURITY

Make the effort for cyber insurance

For heavily regulated businesses, such as the banking sector, data breaches are also a compliance risk because of the potential fines, penalties, and reputational damage that follow a major, public leak. Many organizations seek to cover potential losses with insurance, but the requirements to secure adequate coverage can be challenging.

Insurers typically look at the quality of the defense technology an organization has invested in, how well cyber defenses have been implemented in practice, and how well staff are trained and educated across the business, said a CAE from the insurance industry in the Philippines. She added that a major factor in cyber defense failures is "people risk," and mandatory training is seen as critical, as are high levels of cyber awareness among executive management and the board. A CAE at a bank in the Philippines said he set up cybersecurity workshops for senior members of the organization's board, audit, and risk committees to raise awareness and keep them engaged at a strategic level.

Educate about risks from AI

Finally, generative AI, such as ChatGPT and Google Bard, poses a new kind of cybersecurity threat. These tools entice users with the ability to generate various kinds of content and the ability to write computer code. However, these advantages come with vulnerabilities.

"The evolving use of artificial intelligence has amplified the increasing level of cyberattack and cyber warfare risks," said Melanie Tolentino Oteyza, Group CAE of Meralco in the Philippines.

A CAE based in Singapore said, "We were shocked with the introduction of these programs because, on the one hand …they provide useful solutions, but they can accidentally put out a lot of confidential data on the business when we do not know what people are doing with it."

Thousands of ChatGPT accounts were compromised between June 2022 and May 2023, and the Asia Pacific region accounted for about 40% of them, according to research by Group IB.[2]

Resources

Assessing Cybersecurity Operations: Prevention and Detection (The IIA)

The IIA's Three Lines Model (The IIA)

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

In response, CAEs must stay diligent about the governance processes around the latest technology adopted by the organization. That means ensuring guidelines and policies exist and that management adheres to them – despite the ease with which programs can be deployed and used.

[2] For more about compromised ChatGPT accounts, see https://www.group-ib.com/media-center/press-releases/stealers-chatgpt-credentials/

CYBERSECURITY

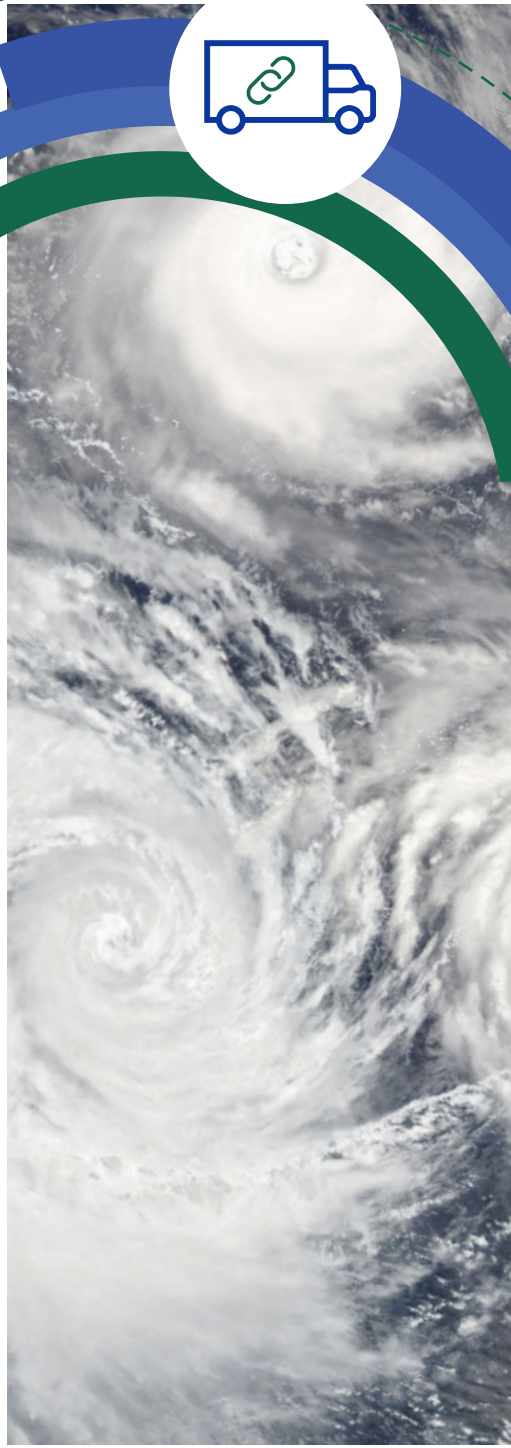
How internal audit can help the organization

1. Identify mission-critical systems and data; understand layers of protections and their dependency on external vendors.
2. Take a holistic view of cybersecurity defenses implemented by different internal and external assurance functions and look for gaps and duplications.
3. Assess staff awareness and alertness on cyber safety across the business, on top of the framework covering prevention, detection, monitoring, response, and recovery processes.
4. Stay abreast of adoption of the latest technologies to timely evaluate the organisation's controls over emerging technologies, such as Chat GPT.
5. Integrate reviews of related critical areas like cybersecurity and business continuity to help strengthen the essential link between these areas.

BUSINESS CONTINUITY

Building operational resilience

In the past, business continuity plans gathered dust on the top shelf. Now organizations are using them to help with strategic decision making and boost organizational resilience.



Given the unprecedented global turmoil since the pandemic began to lock down societies in 2020, businesses in Asia Pacific have been focusing on survival. The pandemic, followed by soaring prices and higher interest rates, have created rapid changes in global and regional markets and pushed some organizations to the brink.[3] Complexity and unpredictability loom large.

But CAEs at the regional roundtable said they were adopting a proactive stance. "Our biggest emerging risk is the ability of every part of the organization to critically identify what-can-go-wrong scenarios even before risks hit," said a CAE of a Philippines-based electronics company. Other CAEs agreed that the issue had risen up the agenda in their boardrooms and among the many family-owned businesses in the region.

Resources

Auditing Third-Party Risk Management (The IIA)

Business Continuity Management (The IIA)

Survey Results – Business Continuity

2ND – RISK LEVEL
61% ranked it as a top 5 *for risk level*

2ND – AUDIT EFFORT
59% ranked it as a top 5 *for audit effort*

[3] For more about insolvency trends, see https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/economic-research/publications/specials/en/2023/april/2023_04_11_Insolvency-Report_AZ.pdf

BUSINESS CONTINUITY

Re-assess continuity plans

The focus for business continuity planning is on proactive, practical plans. In view of the pandemic and geopolitical tension, organizations are rethinking business models and restructuring supply chains. A CAE at a major Taiwanese bank said that businesses in Taiwan were hurrying to create shorter supply chains and to diversify their customer base to become less dependent on mainland China. He said ISO 22301 has become a key tool in enabling organizations to create detailed, testable plans that they can use for strategic decision making.[4]

One Sri Lankan-based CAE said her board used risk software to identify key risks, examine mitigation efforts, and target controls testing. Line managers at that organization were banned from using consultants to create business continuity plans so that the first line both owned the risk and could test the viability of the plan through tabletop exercises. Gone are the days when business continuity plans sat on a shelf gathering dust.

Identify interconnected risks

For countries like Sri Lanka, macroeconomic and geopolitical uncertainty are key drivers. Such risks are unpredictable, dynamic, and hugely interconnected with other threats, CAEs at the roundtable said. For business continuity risk management, that means identifying and mitigating not just individual risks, but the connections between risks, which can be difficult to spot and understand. Working closely with other assurance functions, such as enterprise risk management, is key so that the emerging risk universe is robust, and issues are communicated throughout the business.

Ultimately, business continuity efforts must focus on improving overall organizational resilience, rather than on tackling risks in isolation. In 2022, for instance, Sri Lanka faced the worst economic crisis since independence in 1948 and a collapse of government. There was no fuel, and riots brought the country to a standstill. Prasenna Balachandran, CRO at LAUGFS Holdings in Sri Lanka, said that the situation led his organization to rethink what business continuity planning meant.

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

BUSINESS CONTINUITY

"It is the job of internal auditors and risk managers to train our organizations to face any type of challenge, rather than focusing on a few narrow ones," Balachandran said. To plan more broadly for the future, at his organization, first-line managers are required to create business continuity plans with three different scenarios based on the organization's risk assessment. As the chief risk officer, Balachandran changes the scenarios each year so that, over time, the business continuity plans act as a training ground to help strengthen resilience from any challenge. Internal audits of the first line ensure the business continuity plans are properly practiced, and performance is reported to the board.

Use leading risk indicators

Internal audit can also help organizations identify leading risk indicators that flag potential hotspots before they hit. Too many businesses take the easier route of monitoring lagging indicators that relate to past problems in their business continuity plans, said a CAE from a Sri Lankan bank.

CAEs can help their organizations focus on developing leading risk indicators by looking at the root cause of audit findings in areas where failures are evident. For example, a Singapore-based CAE at the roundtable said he had found that people behind certain control weaknesses were not trained to deal with the uncertainties they faced, especially since many senior level staff had left the organization. Instead of blaming the failures on poor supervisory practices, the CAE recommended that management define leading risk indicators based on the percentage of staff that needed to be trained in those areas.

Supporting the first and second lines with more empathetic internal auditing that seeks to understand how and why gaps or problems have arisen is an imperative to build trust and cooperation so the three lines can act as a team. Given that many organizations in the region have increased automation efforts to reduce skills shortages, embedding controls within automated operating processes also enhances resilience.

CAEs can help their organizations focus on developing leading risk indicators by looking at the root cause of audit findings…

Strengthen governance

Survey respondents ranked governance/corporate reporting as the second highest area of effort for internal auditors (see Figure 2). Some of that effort is going into business continuity planning. For example, Melanie Tolentino Oteyza, Group CAE at Meralco in the Philippines, worked closely with ERM in the organization to identify new and emerging threats and interrelated risks and to update the risk universe. Audit engagements were carried out to review the business continuity plans of various functional units, and new governance processes were recommended, which included creating

BUSINESS CONTINUITY

a working committee for business continuity and resilience.

Oteyza said live tabletop exercises for business continuity and resilience have been instrumental in improving the interdependency between the first and second lines within the organization. In addition, reviewing the interdependencies between the three lines can reveal any redundancies in business continuity plans and any areas where specific responsibilities have been unassigned.

"We do tabletop exercises, too, where we observe and offer recommendations to strengthen resiliency in those processes," she said. This audit exercise can also help improve building data integrity and data flows throughout the business – a process that, once completed, can reduce the cycle time for internal audit work.

Three years from now, survey respondents still expect business continuity to be the second highest risk organizations face in Asia Pacific, and it will remain a key area of focus for internal audit effort as well (see Figures 6 and 8). Boosting the diversity of skills needed

Three years from now, survey respondents still expect business continuity to be the second highest risk organizations face in Asia Pacific, and it will remain a key area of focus for internal audit effort as well.

for internal audit is a major task given the human resources challenges that have impacted the region, especially for specialist technical domains and public sector organizations. CAEs at the roundtable said they were increasing staff training to expand skills in their departments, especially where money was tight. They also said they had networked more in the last couple of years with colleagues in related industries and at IIA regional chapters to share knowledge and best practices.

BUSINESS CONTINUITY

How internal audit can help the organization

1. Evaluate whether business continuity plans are up-to-date, relevant, and realistic, including how well they consider the impact of emerging risks on supplier chain management and nth party risk.
2. Assess how well the three lines collaborate to identify, monitor, and mitigate interconnected risk so that risks and responses are not siloed but considered holistically.
3. Help organizations identify leading risk indicators (that flag out potential hotspots before they hit) through connecting the dots of internal audit's multiple access points in the organisation.
4. Continue to enhance internal audit skills related to business continuity planning through internal training and experience-sharing with practitioners in related industries.

HUMAN CAPITAL

Adjusting to the new reality for talent

When workers move to higher-paid opportunities in neighboring countries, organizations are automating processes, realigning human resource strategies, and getting creative. In addition, employees' ideas on "work" and "life" have rapidly evolved.

While all areas of Asia Pacific have been hit with human capital challenges, the causes are diverse across the countries and industries in the region. CAEs at the region's roundtable said that unlike North America and Europe, they had been less affected by the so-called Great Resignation (an exodus of experienced, older staff looking for a change of lifestyle following the pandemic).[5] But their organizations had been more vulnerable to macroeconomic and geopolitical changes in neighboring countries.

For example, during the pandemic, many skilled foreign workers left Singapore, returned to their home countries, and did not come back after the pandemic eased, leaving critical roles unfilled. In the Philippines and Sri Lanka, higher wages in neighboring countries lured key workers away from the domestic market. In most countries, inexperienced interns were filling the gaps with mixed results, while experienced staff were increasingly likely to switch jobs.[6]

Survey Results – Human Capital

3RD – RISK LEVEL
59% ranked it as a top 5 *for risk level*

7TH – AUDIT EFFORT
33% ranked it as a top 5 *for audit effort*

[5] For more about the Great Burnout, see https://theconversation.com/the-great-resignation-didnt-happen-in-australia-but-the-great-burnout-did-201173

[6] For more about talent strategy in Asia, see https://asia.nikkei.com/Economy/The-post-COVID-Great-Resignation-comes-to-Asia-Hays-CEO

HUMAN CAPITAL

A shortage of IT and cybersecurity specialists created by rapid digitalization has seen wage inflation hit between 60% and 70% for some roles, according to a CAE at an Indonesian bank. "In Indonesia, we only have about 400 certified information system auditors for the whole country, and last year the regulator introduced heightened regulatory requirements for cybersecurity maturity assessment, data protection, and so on," he said. "That is causing big banks, start-ups, fintech firms, and others to poach the limited resources in this space."

Strategy for talent pipelines

Many roundtable attendees said businesses were hurrying to harness technologies such as automation and digitalization – if they can attract and retain the staff to do so. That has eased pressure in those parts of their organizations that depend on low-skill, high-transaction processes. But it has also hollowed out traditional entry-level jobs, said a CAE from Australia, leaving businesses struggling to recreate sufficient early career roles to fill their talent pipelines.

That problem was made worse by the pandemic as global organizations escalated their use of shared service centers in their regional operations, for example, to perform enterprise-wide administrative tasks. That has not only failed to help them retain key personnel, but has also consolidated new entry-level talent for those roles in fewer countries, such as Vietnam and Malaysia.[7]

"We have been automating to cut headcount at the same time as seeking to overcome staff turnover by creating attractive incentive packages for high-potential staff – one that is backed up with a well-defined career path that we hope will bind them to the organization," said Prasenna Balachandran, CRO at LAUGFS Holdings in Sri Lanka. While that has helped, he said, the pressure on more senior staff has grown as they juggle their own responsibilities while mentoring junior employees – increasing the risk of burnout. Given that many skilled staff have left the country for Australia and Canada after three years of economic and political turmoil, retaining remaining talent is critical.

Resources

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

Cultivating a Healthy Culture (Chartered Institute of Internal Auditors)

2023 Organizational Culture and Ethics Report (Audit Board)

Corporate culture

Auditing hard controls around, for example, payroll and the accuracy of employee records, is important but does not address today's dynamic labor market, CAEs at the roundtable said. While audit automation has increasingly taken care of compliance checks, tackling cultural changes accelerated by the pandemic can add additional value.

[7] For more about challenges related to shared services, see https://cn.accaglobal.com/content/dam/acca/news/files/40.%20Future%20challenges%20facing%20the%20Shared%20Services%20Centre%20in%20China%20and%20greater%20Asia%20Pac ific.pdf

HUMAN CAPITAL

In Japan, for instance, the long-term trend of working in a single company for life is waning. Companies suddenly find themselves having to create career structures for middle managers. That has challenged every assumption that those human resources departments have embedded in their processes, a CAE from a Japanese electronics business said. Working with the first and second lines to help brainstorm solutions and offer supportive criticism was welcomed by management.

Internal audit has a role when they are well-focused on specific problems, and a short, targeted audit can help. For example, A CAE from an Australian industrial business did a special audit to explore drops in retention rates after parental leave and discovered that the characteristics of the supervisor played a key role. “If we had taken a simply transactional approach, we would have missed some key metrics,” she said, suggesting that adopting a more considered, detailed, and analytical approach is key.

In terms of human capital challenges, internal audit departments have been hit as hard as the organizations they serve – sometimes harder… Many at the roundtable said internal audit employee counts were down.

But organizations must also ensure that they strengthen their corporate culture and that it is in line with recent trends and developments. CAEs have a key role to play in coordinating across the enterprise to effectively assess, monitor, and embed positive organizational culture. That should include ensuring that employee survey data is regularly collected and acted upon and that they align with what the business most needs to know.

Filling internal audit skills gaps

In terms of human capital challenges, internal audit departments have been hit as hard as the organizations they serve – sometimes harder. As well as suffering from the same skills shortages in areas such as cybersecurity and IT, internal audit is experiencing shortages in traditional skill sets such as accounting. For example, CPA exams in the Philippines were canceled during the pandemic, significantly reducing the number of people graduating as accountants, a roundtable participant noted. Attracting suitably qualified new starters is tough.

Many at the roundtable said internal audit employee counts were down – one was two-thirds lower than what was needed. Fortunately, she had developed an automated auditing platform in conjunction with the finance

HUMAN CAPITAL

team in 2018, which had helped plug the shortfall. If retention is difficult, finding replacement staff can be harder, especially for public sector and for all but the biggest organizations. Other CAEs said they had been using ChatGPT, for instance, to help less technical internal auditors write code for analyzing data and improving risk assessments, but with increased cyber risk from such new technologies, there are dangers to such an approach.

A CAE at a Philippines-based retail business said that along with co-sourcing internal audit services from consultancy firms, he has enticed colleagues out of retirement to help on assignments where they have high levels of expertise. In addition, he initiated an educational campaign among risk owners to strengthen their controls culture and awareness. A CAE at an Indonesian bank said he had brought subject matter experts into the internal audit team to bolster his team's expertise, as well as seconded his cybersecurity internal audit expert to the first line to improve their controls and risk awareness.

> "The real challenge now is performance over conformance in terms of enhancing the value of internal audit."

In most Asian countries, stock exchange listing rules mandate internal audit in public companies. While this regulatory push has raised the profile of the profession and created better standing and job security for internal auditors, the real challenge now is performance over conformance in terms of enhancing the value of internal audit. Where environmental, social, and governance (ESG) regulations are becoming compulsory, they can also be a driver to attract fresh talent, but CAEs emphasized the need to communicate an organization's sustainability purpose and goals clearly throughout the business and in human resources policies and procedures.

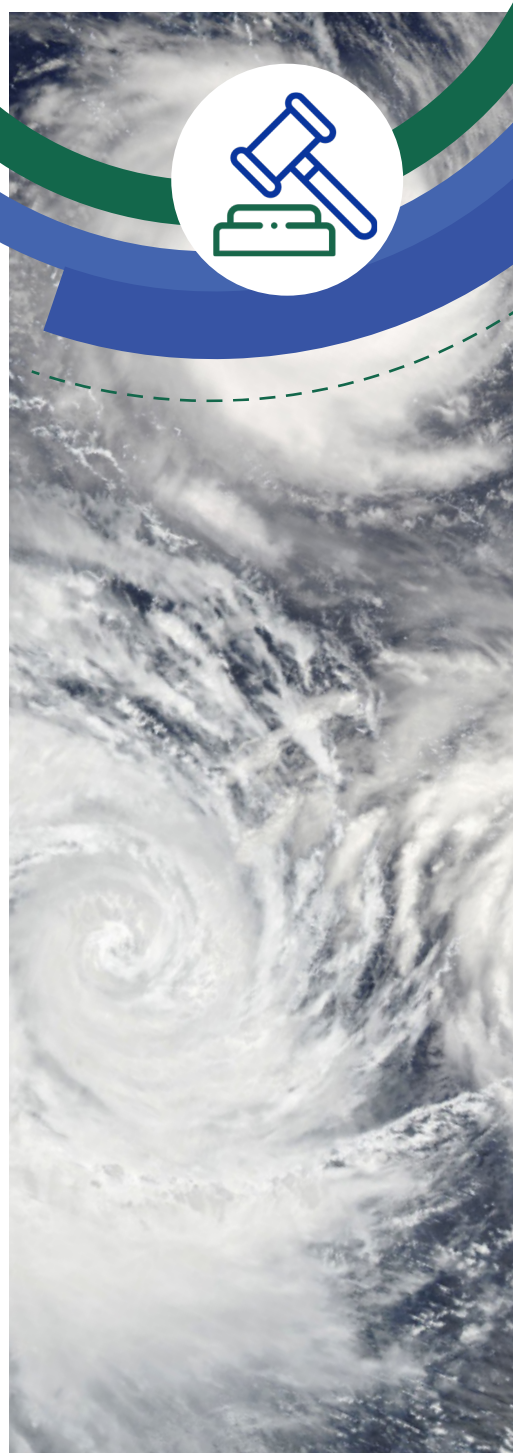
HUMAN CAPITAL

How internal audit can help the organization

1. Understand factors affecting the organization's talent management, including the effect of technologies, strategy for entry-level positions and career structures, to timely assess the impact on the organization and internal audit respectively
2. Assess the effectiveness of the organization's human capital strategies and management processes in light of macro-factors reshaping the labor market and changing employee expectations.
3. Evaluate the effectiveness of not only hard controls (such as structure, policies, and processes), but also soft controls (such as corporate culture and employee survey communications).
4. Provide advisory services, such as training and facilitation workshops, to help promote staff control awareness and the organization's core values, apart from assurance services.
5. Use internal audit as a training ground for the organization's future management personnel through guest audit program and secondment of internal audit staff to other functions.

REGULATORY CHANGE

Taking a strategic approach to compliance



Given the highly connected trading relationships between countries in the Asia Pacific region, regulatory compliance is a major challenge. With a growing tide of data protection laws and new mandatory ESG disclosure requirements, internal audit must take a strategic approach to compliance.

New data protection laws

Major economies in Asia Pacific are adopting modified versions of Europe's 2018 General Data Protection Regulation to protect citizens' personal data. But they are doing so differently. China, for example, recently amended its 2021 Personal Information Protection Law (PIPL) to restrict the transfer of personal data outside the country.[8] India's draft Digital Personal Data Protection Bill, 2022 takes a softer approach, particularly in light of the use and transfer of data from India.[9] But multiply those differences among all of the other similar regulations in the region, and it is easy to see why organizations are struggling.

A healthy organization evolves like a living organism and continuously adapts to the changing environment, said Helen Li, CAE at The Bank of East Asia. She says internal audit's work is not just to assess an organization's "healthiness"

Survey Results – Regulatory Change

5TH – RISK LEVEL
35% ranked it as a top 5 *for risk level*

3RD – AUDIT EFFORT
56% ranked it as a top 5 *for audit effort*

[8] For more about China's data law, see https://www.reuters.com/world/china/chinas-steps-control-its-data-information-2023-05-09/
[9] For more about India's data protection law, see https://iapp.org/news/a/indias-proposed-digital-personal-data-protection-bill-arrives-before-parliament/

REGULATORY CHANGE

at a particular point in time or just for specific regulations. "Taking regulatory compliance as an example, checking observance with individual rules is not effective because there are too many," Li said. "The business, your products, and regulatory requirements are constantly changing, so you must assess the control framework in place and make sure your organization has a very robust mechanism to keep up with the changes and adapt where necessary."

Urgent action for ESG

CAEs at the roundtable said ESG reporting will become one of the biggest compliance struggles of the next few years. Survey respondents also indicated dramatic increases in internal audit effort related to climate change, biodiversity, and environmental sustainability in the next three years (see Figure 8). The gold standard for ESG disclosures has primarily been set by Europe following the creation of international standards by the Netherlands-based Global Reporting Initiative and the UK's Task Force on Climate-related Financial Disclosures.

CAEs at the roundtable said ESG reporting will become one of the biggest compliance struggles of the next few years.

Compulsory regulations based on those rules are now in place in the European Union (EU).[10] Those will have an effect on suppliers to Europe operating in Asia Pacific, especially when a related supply chain directive comes into force that will require European businesses to prove that their suppliers behave in environmentally and socially protective ways.[11] Those that do not may be unable to provide goods and services to Europe.

Countries such as India, Japan, and Singapore are following suit by creating mandatory reporting rules based largely on such requirements.[12] Other Asia Pacific countries have so far adopted more of an advisory stance for stock exchange disclosure rules, but as pressure grows for greener businesses from investors and consumers, mandatory regulation is likely.

Many global organizations in the region have started preparing for the change (along with some smaller publicly listed firms), but others need to make more headway on this issue. For example, Stephen Ching, governor of IIA–Singapore, commented: "CAEs are obviously not in a position to audit something that does not exist, so they need to seriously engage directors and highlight to them that this is now a requirement of the Singapore Stock Exchange and that the business must get ready."

Even in those companies further along in the journey, there is still work to be

[10] For more about corporate sustainability reporting from the EU, see https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en
[11] For more about the new supply chain rules, see https://www.elevatelimited.com/blog/eu-parliament-approves-supply-chain-due-diligence/
[12] For more about ESG rules in Asia Pacific, see https://newsdirect.com/news/esg-disclosure-regulations-are-strengthening-in-asia-pacific-781581983

REGULATORY CHANGE

done. Ching said that because of the large amounts of data that ESG reports need to collate, CAEs can consider adopting continuous auditing methodologies to keep ahead. "Engage the business from the start, know the framework, understand the source of data and whether it is complete. Because it is a new area, there is a lot of room for improvement in these places, even among higher-capitalized companies," Ching said.

Preventing greenwashing

Greenwashing is a growing concern in Asia Pacific, as misleading or bogus sustainability claims are used to attract customers, investments, or even employees.[13] "Companies are finding that it is essential to promote ESG, which is also about diversity, and capturing and retaining talent," a CAE from a Japanese multinational said.

Strong assurance over ESG reporting will prevent greenwashing – or accusations of it, which can be equally harmful. Such charges can damage reputations and lose organizations business, on top of the compliance repercussions. Internal audit will have to work hard to provide assurance that ESG claims used in corporate communications are accurate and complete, considering the wide range of data used and different levels of data governance maturity.

Greenwashing is a growing concern in Asia Pacific, as misleading or bogus sustainability claims are used to attract customers, investments, or even employees.

[13] For more about reenwashing in Asia Pacific, see https://www.eco-business.com/news/the-next-wave-of-green-washing-offsets-competitor-claims-and-transition-washing/

REGULATORY CHANGE

How internal audit can help the organization

1. Stay on top of the latest regulatory requirements and emerging risk areas, such as greenwashing, to timely adjust audit focus and approach.
2. Be aware of the impact of regulatory requirements from all of the relevant jurisdictions to assess impact of complicated areas, such as compliance with data sovereignty rules.
3. Develop a good understanding of the organization's regulatory compliance framework and processes covering entity-level, business-related, and location-specific controls. Identify better practices for sharing, apart from control improvement opportunities.
4. Evaluate the effectiveness of the control framework in place for regulatory compliance, including the organization's ability to respond to fast-changing regulatory developments.

ACKNOWLEDGEMENTS

Asia Pacific Report Development Team

Asia Pacific regional liaison
Stephen Coates –
President, ACIIA (Asian Confederation of Institutes of Internal Auditors)

Roundtable moderators
Helen Li –
Group Chief Auditor, The Bank of East Asia, Hong Kong China
Sue Ironside –
General Manager Internal Audit Area of Expertise, Rio Tinto, Australia
Nam-Chie Sia –
Head of Risk Management, Legal and Compliance, Hong Leong Finance, Singapore

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/foundation