

# 2025

## RISK IN FOCUS

Hot topics  
for internal  
auditors

[Read More](#)

# INDONESIA



Internal Audit  
**FOUNDATION**



Asian Confederation of  
**Institutes of Internal Auditors**

# ABOUT GLOBAL RISK IN FOCUS

## Know your risks. Plan strategically.

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

Using survey results and regional roundtables, Risk in Focus reveals key insights from internal audit leaders worldwide about:

- Current risk levels and audit priorities.
- Risk level changes in the past year.
- Risk drivers per region.
- Leading practices for addressing top risks.

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. The Foundation gratefully acknowledges the participation of all IIA regional bodies:

- African Federation of Institutes of Internal Auditors ([AFIIA](#))
- Arab Confederation of Institutes of Internal Auditors ([ARABCIIA](#))

- Asian Confederation of Institutes of Internal Auditors ([ACIIA](#))
- European Confederation of Institutes of Internal Auditors ([ECIIA](#))
- Fundación Latinoamericana de Auditores Internos ([FLAI](#))

Risk in Focus was originally created in 2016 by the European Institutes Research Group (EIRG), which continues to publish the report in Europe through the ECIIA.

Designed as a resource for internal auditors and their stakeholders, Risk in Focus will spark conversations and bring new insights to risks that impact your organization, and the world.

Risk in Focus reports and presentations are available for free at the [Risk in Focus Knowledge Center](#).



Internal Audit  
FOUNDATION

Visit the [Risk in Focus Knowledge Center](#) to download free reports and summary presentations to share with stakeholders.

### RESEARCH PARTICIPATION WORLDWIDE

124  
countries/  
territories

3,544  
survey  
responses

18  
roundtables with  
138  
participants

27  
in-depth  
interviews



# CONTENTS

<b>4</b>	Executive Summary – Indonesia
<b>5</b>	Introduction
<b>7</b>	Survey Response Rates
<b>8</b>	Global – Risk Trends
<b>9</b>	Indonesia – Risk Trends
<b>14</b>	Indonesia – Risk in Focus
<b>18</b>	Digital Disruption
<b>20</b>	Internal Audit Foundation Partners
<b>21</b>	About The IIA



# EXECUTIVE SUMMARY – INDONESIA

## Proactive advisors to face challenges

Cybersecurity, digital disruption (including AI), business continuity, and climate change remain to be the risks need to be mitigated in Indonesia in the next three years. A bit different with Asia Pacific and worldwide, where climate change, beside digital disruption (including AI), is expected to be the fastest climbing risk.

After series of election in 2024, Indonesia will navigates through new government in 2025. Indonesia Risk in Focus 2025 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?
- How internal audit focus may change in the future?
- Which areas that will be negatively impacted by artificial intelligence?

In 2025, it is expected that top risks in Indonesia are cybersecurity, fraud, business continuity, digital disruption (including AI), and regulatory change.

In near future those risks most likely will change since people will be more alert on climate change and geopolitical uncertainty than fraud and regulatory change.

Indonesia is a very large country and has unique geographical conditions. It means digital disruption is an inevitability that cannot be avoided. Technological progress has its own challenges but also provides wide open opportunities. Internal auditors in Indonesia need to be proactive as advisors for strategic success and facing tough challenges. Effective communication with both management and board will have great importance to successfully executing internal audit assignments.

### ASIA PACIFIC REPORT SPONSORS



Asian Confederation of  
**Institutes of Internal Auditors**

- IIA–Australia
- IIA–Hong Kong, China
- IIA–Indonesia
- IIA–Japan
- IIA–Philippines
- IIA–Singapore
- IIA–Chinese Taiwan



## INDONESIA RESEARCH PARTICIPATION

# 87

survey responses  
from CAEs and directors

# INTRODUCTION

## Risk drivers for emerging risks

Based on discussions with audit leaders around the world, six risk drivers were identified as key elements that influence how internal audit leaders rank and respond to risks. These were divided into two types – direct pressure and indirect pressure.

The risk drivers that create direct pressure were regulations, financial impact, and business opportunity. These have a strong influence on how the board sets priorities and internal audit scope, particularly in the short term.

Indirect risk drivers — politics, public opinion, and social impact — may take longer to influence risk levels at the organizational level. However, indirect pressure may ultimately lead to direct pressure. For example, political priorities can lead to regulations, while public opinion can turn into market pressure. In addition, social impact can lead

to new priorities for both the public and private sector. The interplay between direct and indirect pressure creates long-term influence on risk levels and audit priority.

During Risk in Focus roundtables and interviews, these risk drivers were evident in how organizations worldwide approach climate change and digital disruption (including AI). Awareness of these risk drivers can help internal audit leaders and their stakeholders with short-term and long-term strategic decision-making.

## Risk Drivers for Emerging Risks

**Regulations**  
Specific regulations and consequences for noncompliance

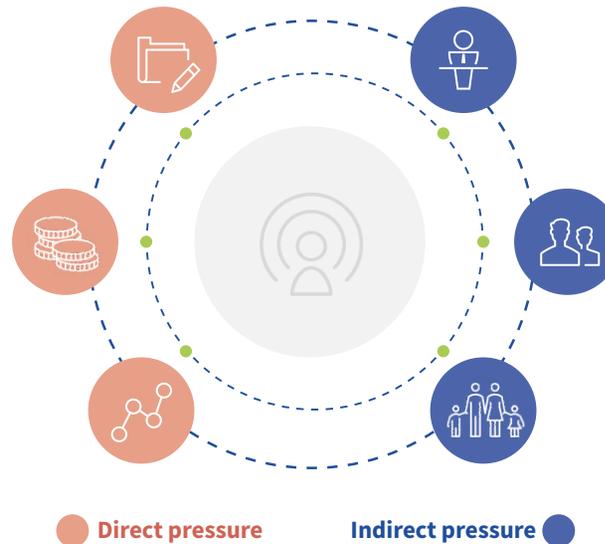
**Financial impact**  
Impact on revenues or assets (including fraud)

**Business opportunity**  
Advantage for business, or risk of falling behind

**Politics**  
Political priorities or trends related to the risk area

**Public opinion**  
Pressure from the public, the market/customers, or stakeholders

**Social impact**  
Harm or benefit for people or society in general



# INTRODUCTION

## How we do the research

Each year, Risk in Focus research starts with a survey of CAEs and heads of internal audit to identify current and emerging risks for each region. Results are used to identify areas for follow-up roundtables and interviews with CAEs and other industry experts. The survey focuses on 16 risk categories, shown below.

Respondents were asked two key questions:

- What are the top 5 risks your organization faces?
- What are the top 5 audit areas on which internal audit spends the most time and effort?

To assess risk trends, respondents were also asked about their expectations for risk levels and audit priorities three years in the future.

The global survey for all regions except Europe was conducted from 21 March 2024 to 20 May 2024 and received 2,559 responses. The survey specifically for Europe was conducted from 4 March 2024 to 1 April 2024 and received 985 responses. Combined, the two surveys received in total of 3,544 responses, which 87 of those are from Indonesia. Both surveys were conducted online through contacts associated with IIA institutes and regional bodies.

## Risk Areas Included in the Report

	Risk Name	Risk Description Used in the Survey
1	<b>Business continuity</b>	Business continuity, operational resilience, crisis management, and disaster response
2	<b>Climate change</b>	Climate change, biodiversity, and environmental sustainability
3	<b>Communications/reputation</b>	Communications, reputation, and stakeholder relationships
4	<b>Cybersecurity</b>	Cybersecurity and data security
5	<b>Digital disruption (including AI)</b>	Digital disruption, new technology, and AI (artificial intelligence)
6	<b>Financial liquidity</b>	Financial, liquidity, and insolvency risks
7	<b>Fraud</b>	Fraud, bribery, and the criminal exploitation of disruption
8	<b>Geopolitical uncertainty</b>	Macroeconomic and geopolitical uncertainty
9	<b>Governance/corporate reporting</b>	Organizational governance and corporate reporting
10	<b>Health/safety</b>	Health, safety, and security
11	<b>Human capital</b>	Human capital, diversity, and talent management and retention
12	<b>Market changes/competition</b>	Market changes/competition and customer behavior
13	<b>Mergers/acquisitions</b>	Mergers and acquisitions
14	<b>Organizational culture</b>	Organizational culture
15	<b>Regulatory change</b>	Change in laws and regulations
16	<b>Supply chain (including third parties)</b>	Supply chain, outsourcing, and 'nth' party risk

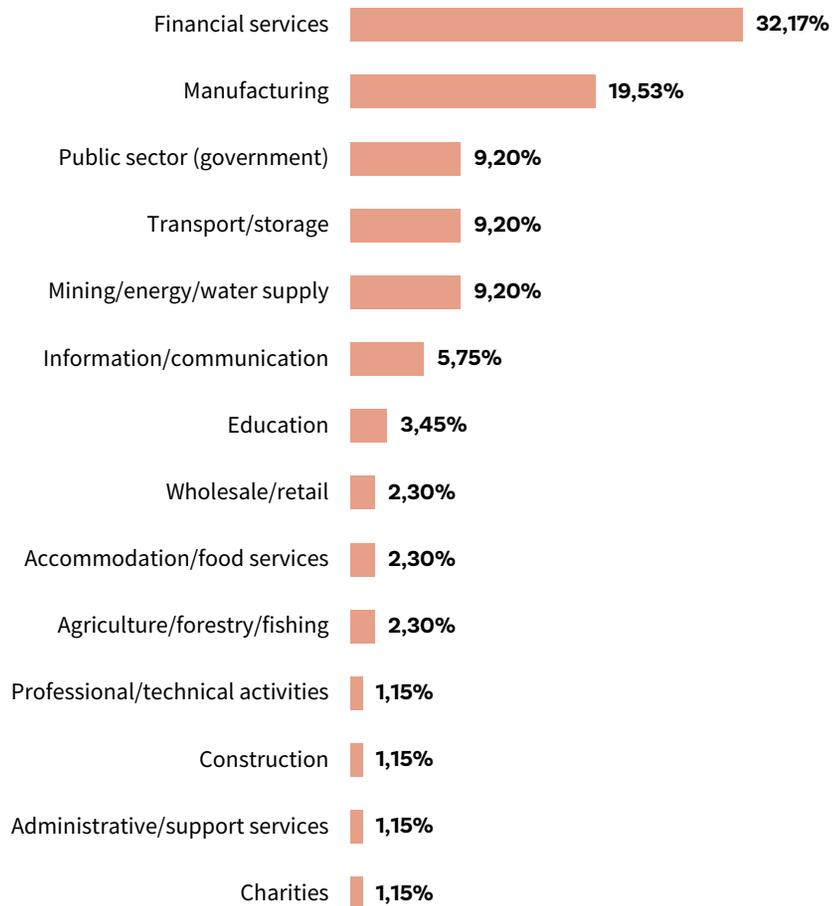


# SURVEY RESPONSE RATES

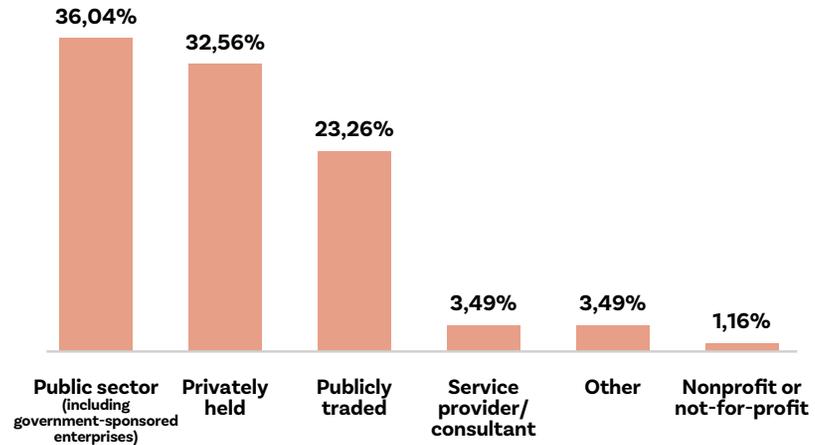
## Indonesia – Demographics

Survey Responses:  
87

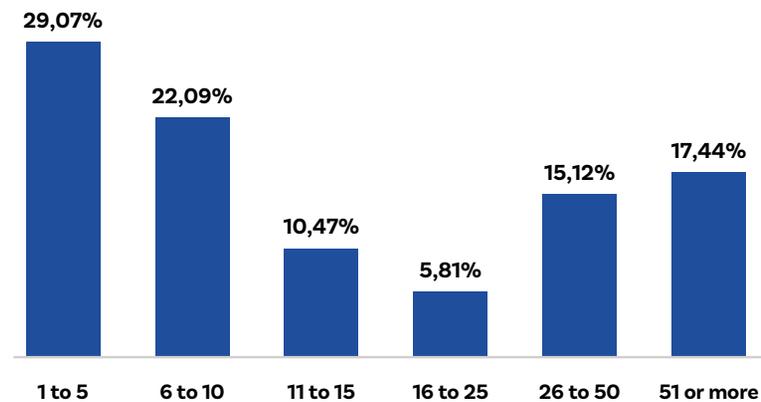
### Indonesia – Industry



### Indonesia – Organization Type



### Internal Audit Function Size (including CAE and sourced staff)



# GLOBAL – RISK TRENDS



Cybersecurity, business continuity, and human capital continue to hold the top three spots in risk rankings. In the next three years, digital disruption is expected to increase 20 percentage points to rank second. At the same time, climate change is expected to increase 16 percentage points to be ranked fifth. None of the other 14 risk areas are expected to see such dramatic changes in ranking or percentages.

## Global – Top 5 Risk Levels – Trend

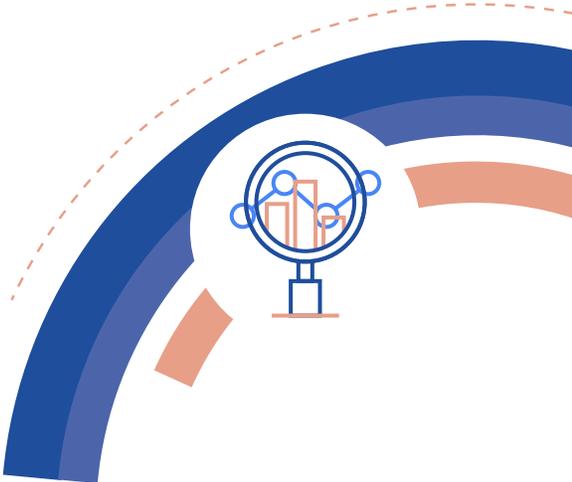
**Survey questions: What are the top 5 risks your organization currently faces? What do you think the top 5 risks will be 3 years in the future?**

Last Year’s Risk		Current Year’s Risk		Risk Expectations in 3 Years	
1. Cybersecurity	73%	1. Cybersecurity	73%	1. Cybersecurity	69%
2. Human capital	51%	2. Business continuity	51%	<b>2. Digital disruption (including AI)</b>	<b>59%</b>
3. Business continuity	47%	3. Human capital	49%	3. Business continuity	47%
4. Regulatory change	39%	<b>4. Digital disruption (including AI)</b>	<b>39%</b>	4. Human capital	42%
<b>5. Digital disruption (including AI)</b>	<b>34%</b>	5. Regulatory change	38%	<b>5. Climate change/environment</b>	<b>39%</b>
6. Financial liquidity	32%	6. Market changes/competition	32%	6. Regulatory change	37%
7. Market changes/competition	32%	7. Financial liquidity	31%	7. Geopolitical uncertainty	31%
8. Geopolitical uncertainty	30%	8. Geopolitical uncertainty	30%	8. Market changes/competition	30%
9. Governance/corporate reporting	27%	9. Governance/corporate reporting	25%	9. Financial liquidity	25%
10. Supply chain (including third parties)	26%	10. Organizational culture	24%	10. Supply chain (including third parties)	24%
11. Organizational culture	26%	11. Fraud	24%	11. Governance/corporate reporting	22%
12. Fraud	24%	12. Supply chain (including third parties)	23%	12. Fraud	21%
13. Communications/reputation	21%	<b>13. Climate change/environment</b>	<b>23%</b>	13. Organizational culture	20%
<b>14. Climate change/environment</b>	<b>19%</b>	14. Communications/reputation	20%	14. Communications/reputation	15%
15. Health/safety	11%	15. Health/safety	11%	15. Health/safety	10%
16. Mergers/acquisitions	6%	16. Mergers/acquisitions	6%	16. Mergers/acquisitions	9%

*Note 1:* The global average is calculated by summing the averages from each region and dividing by the number of regions.  
*Note 2:* Risk in Focus surveys conducted online from 21 March 2024 to 20 May 2024 by the Internal Audit Foundation and the European Institutes Research Group. n = 3,544.



# INDONESIA – RISK TRENDS



Cybersecurity, fraud, and business continuity remain the top three risk rankings in Indonesia. Over the next three years, digital disruption is expected to rise to second place. Meanwhile, although climate change and geopolitical uncertainty are not currently among the top five risks in Indonesia, they are expected to emerge within the next three years, closely followed by regulatory changes.

## Indonesia – Top 5 Risk Levels – Trend

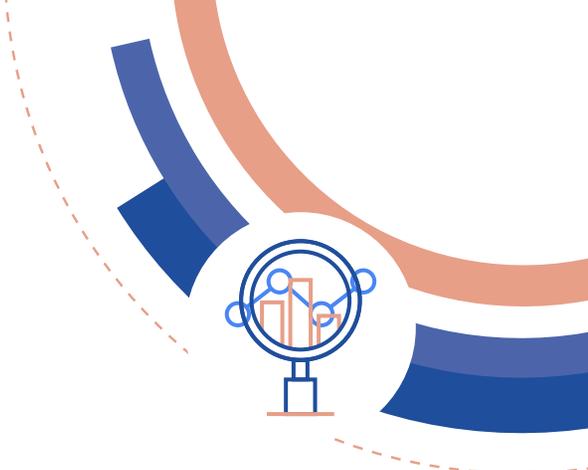
**Survey questions:** Please rank the top 5 risks area your organization is currently facing. How do you think risk may change in the future? Please rank the top 5 risks your organization will face in 3 years time.

Last Year’s Risk		Current Year’s Risk		Risk Expectations in 3 Years	
1. Cybersecurity	60%	1. Cybersecurity	64%	1. Cybersecurity	70%
2. Business continuity	59%	2. Fraud	59%	2. <b>Digital disruption (including AI)</b>	<b>67%</b>
3. Fraud	50%	3. Business continuity	53%	3. Business continuity	51%
4. Regulatory change	48%	4. <b>Digital disruption (including AI)</b>	<b>49%</b>	4. <b>Climate change/environment</b>	<b>43%</b>
5. <b>Digital disruption (including AI)</b>	<b>43%</b>	5. Regulatory change	45%	5. <b>Geopolitical uncertainty</b>	<b>41%</b>
6. Human capital	33%	6. Market changes/competition	34%	6. Regulatory change	40%
7. Organizational culture	28%	7. Financial liquidity	32%	7. Fraud	38%
8. Financial liquidity	26%	8. Human capital	29%	8. Market changes/competition	30%
9. <b>Geopolitical uncertainty</b>	<b>26%</b>	9. Organizational culture	26%	9. Human capital	28%
10. Governance/corporate reporting	22%	10. Communications/reputation	25%	10. Financial liquidity	21%
11. Supply chain (including third parties)	19%	11. <b>Geopolitical uncertainty</b>	<b>24%</b>	11. Organizational culture	17%
12. <b>Climate change/environment</b>	<b>17%</b>	12. <b>Climate change/environment</b>	<b>20%</b>	12. Governance/corporate reporting	15%
13. Health/safety	9%	13. Governance/corporate reporting	18%	13. Communications/reputation	11%
14. Mergers/acquisitions	3%	14. Supply chain (including third parties)	9%	14. Mergers/acquisitions	10%
15. Communications/reputation	-	15. Health/safety	7%	15. Supply chain (including third parties)	9%
16. Market changes/competition	-	16. Mergers/acquisitions	5%	16. Health/safety	9%



# INDONESIA – RISK TRENDS

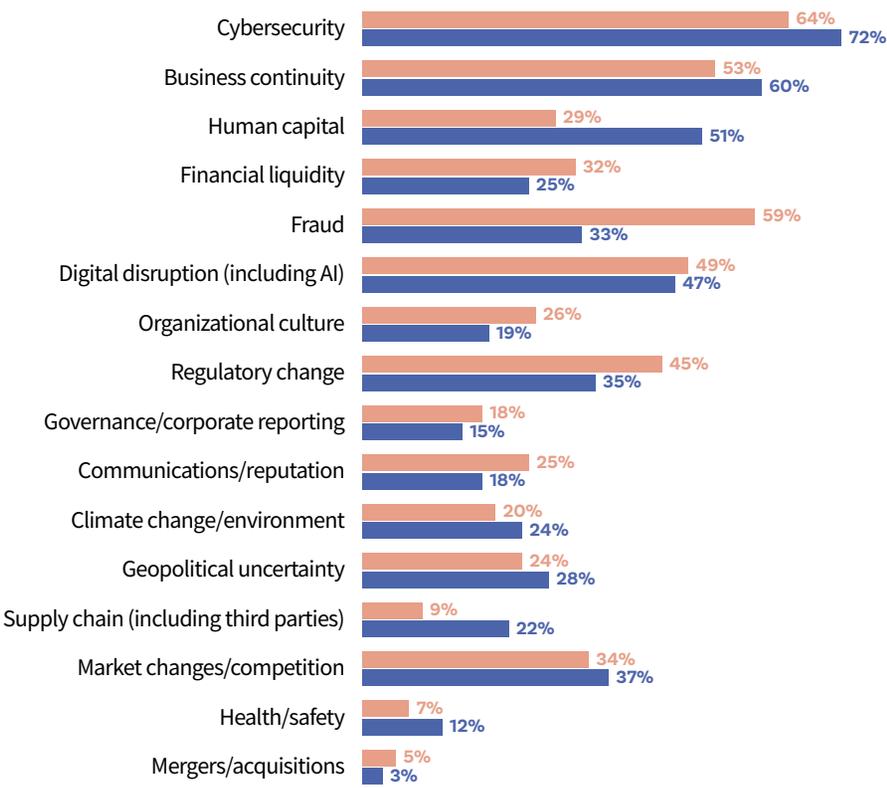
## Survey results – Indonesia & Southeast Asia



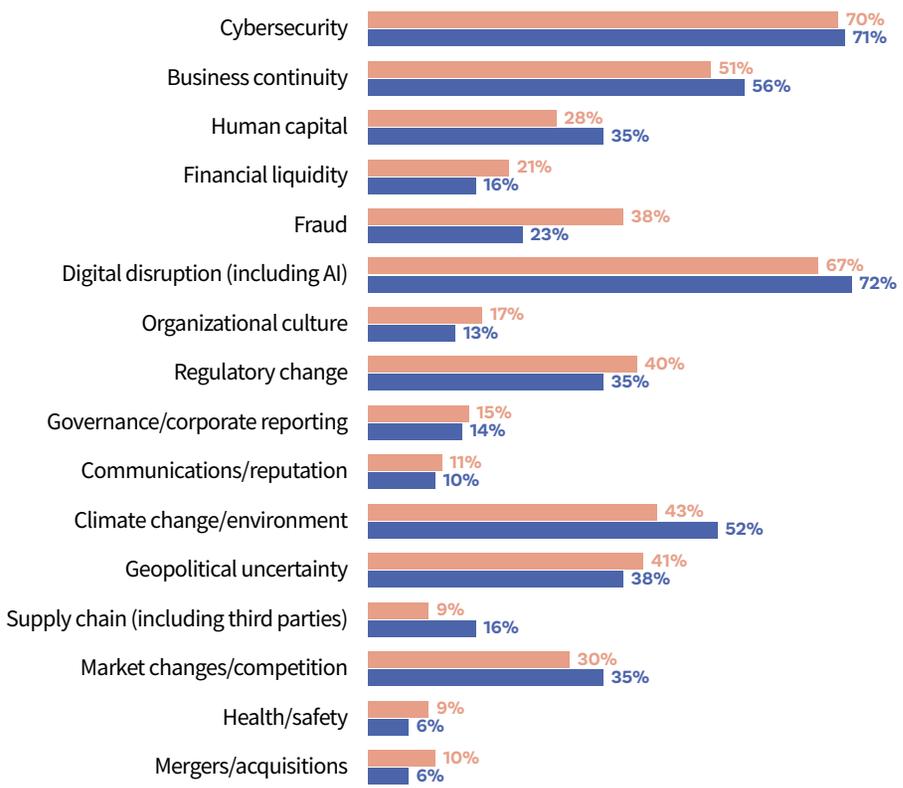
### Current Risk Levels vs. Future Risk Levels

● Indonesia ● Southeast Asia

Current Risk Levels



Future Risk Levels



**Top three risks in 2025 in Indonesia are cybersecurity, fraud, and business continuity. A bit different with the Southeast Asia region, that put human capital instead of fraud in one of their top three risks. In near future, fraud risk is expected to go down on the list, because climate change/environment and geopolitical uncertainty risk are expected to emerge and have higher priority.**

# INDONESIA – RISK TRENDS

## Expected Risks Change in 3 Years - Indonesia

Current Year's Risk			Future Risk		
1.	Cybersecurity	64%	1.	Cybersecurity	70%
2.	Fraud	59%	2.	<b>Digital disruption (including AI)</b>	<b>67%</b>
3.	Business continuity	53%	3.	Business continuity	51%
4.	<b>Digital disruption (including AI)</b>	<b>49%</b>	4.	<b>Climate change/environment</b>	<b>43%</b>
5.	Regulatory change	45%	5.	<b>Geopolitical uncertainty</b>	<b>41%</b>
6.	Market changes/competition	34%	6.	Regulatory change	40%
7.	Financial liquidity	32%	7.	Fraud	38%
8.	Human capital	29%	8.	Market changes/competition	30%
9.	Organizational culture	26%	9.	Human capital	28%
10.	Communications/reputation	25%	10.	Financial liquidity	21%
11.	<b>Geopolitical uncertainty</b>	<b>24%</b>	11.	Organizational culture	17%
12.	<b>Climate change/environment</b>	<b>20%</b>	12.	Governance/corporate reporting	15%
13.	Governance/corporate reporting	18%	13.	Communications/reputation	11%
14.	Supply chain (including third parties)	9%	14.	Mergers/acquisitions	10%
15.	Health/safety	7%	15.	Supply chain (including third parties)	9%
16.	Mergers/acquisitions	5%	16.	Health/safety	9%

### Analysis

#### Digital Disruption

This risk is expected to move up to 2nd (67%) from 4th position (49%) in near future, reflecting the growing impact of AI and technological advancements on business operations.

#### Climate Change/Environment

This risk is expected to climb significantly from 12th (20%) to 4th (43%), indicating increasing awareness and concern about environmental factors affecting businesses.

#### Geopolitical Uncertainty

Currently ranked 11th (24%), this risk is expected to rise to 5th (41%), suggesting heightened instability in global politics and its influence on local and regional markets.

#### Fraud

While it is currently the 2nd highest risk (59%), fraud is expected to drop to 7th (38%) in near future, signaling either in changing risk perceptions or regulatory enforcement in Indonesia may contribute to the decreased urgency around fraud risk.

These shifts demonstrate an evolving risk landscape in Indonesia, with organizations placing greater emphasis on digital, environmental, and geopolitical challenges.

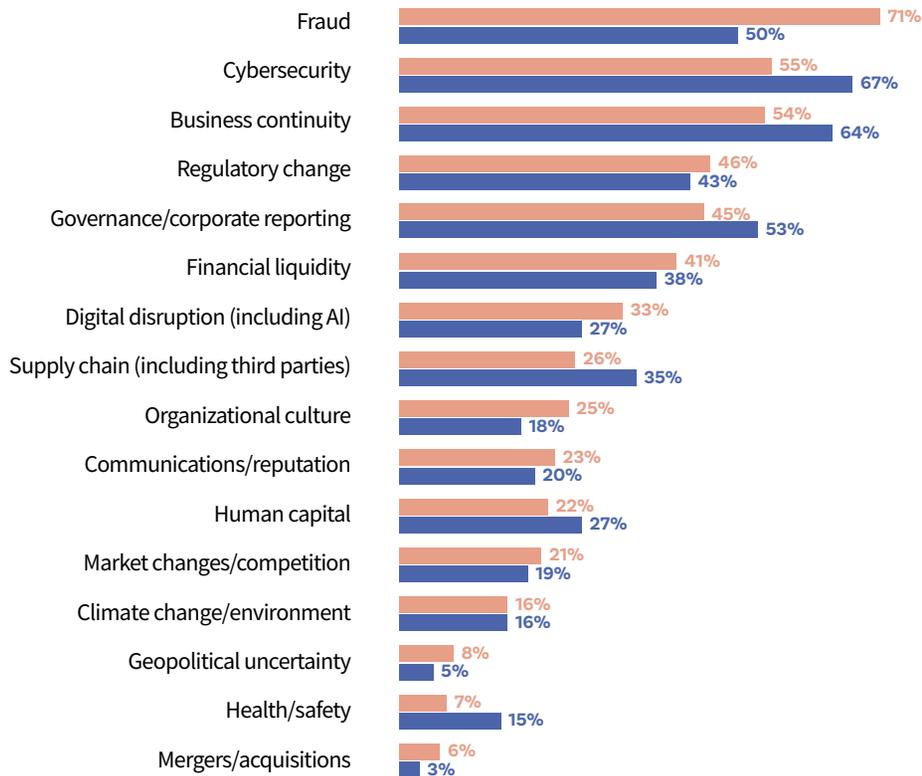


# INDONESIA – RISK TRENDS

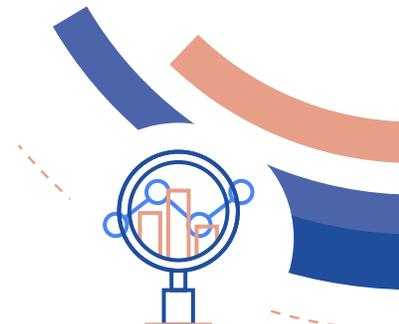
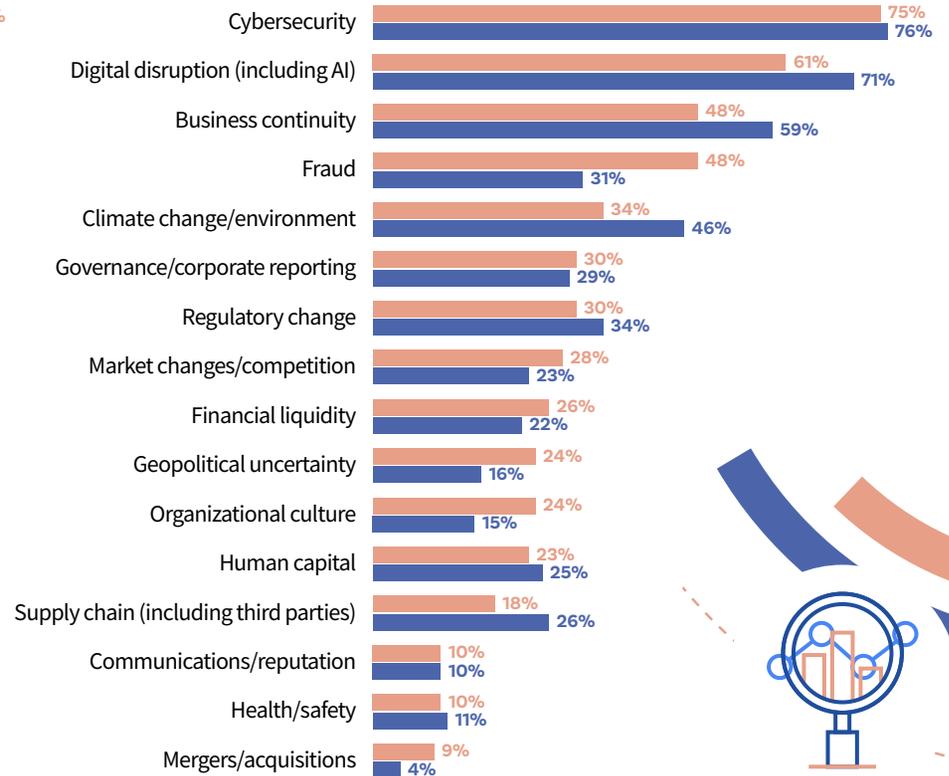
## Current Audit Effort vs Future Audit Effort – Indonesia & Southeast Asia

● Indonesia ● Southeast Asia

### Current Audit Effort



### Future Audit Effort



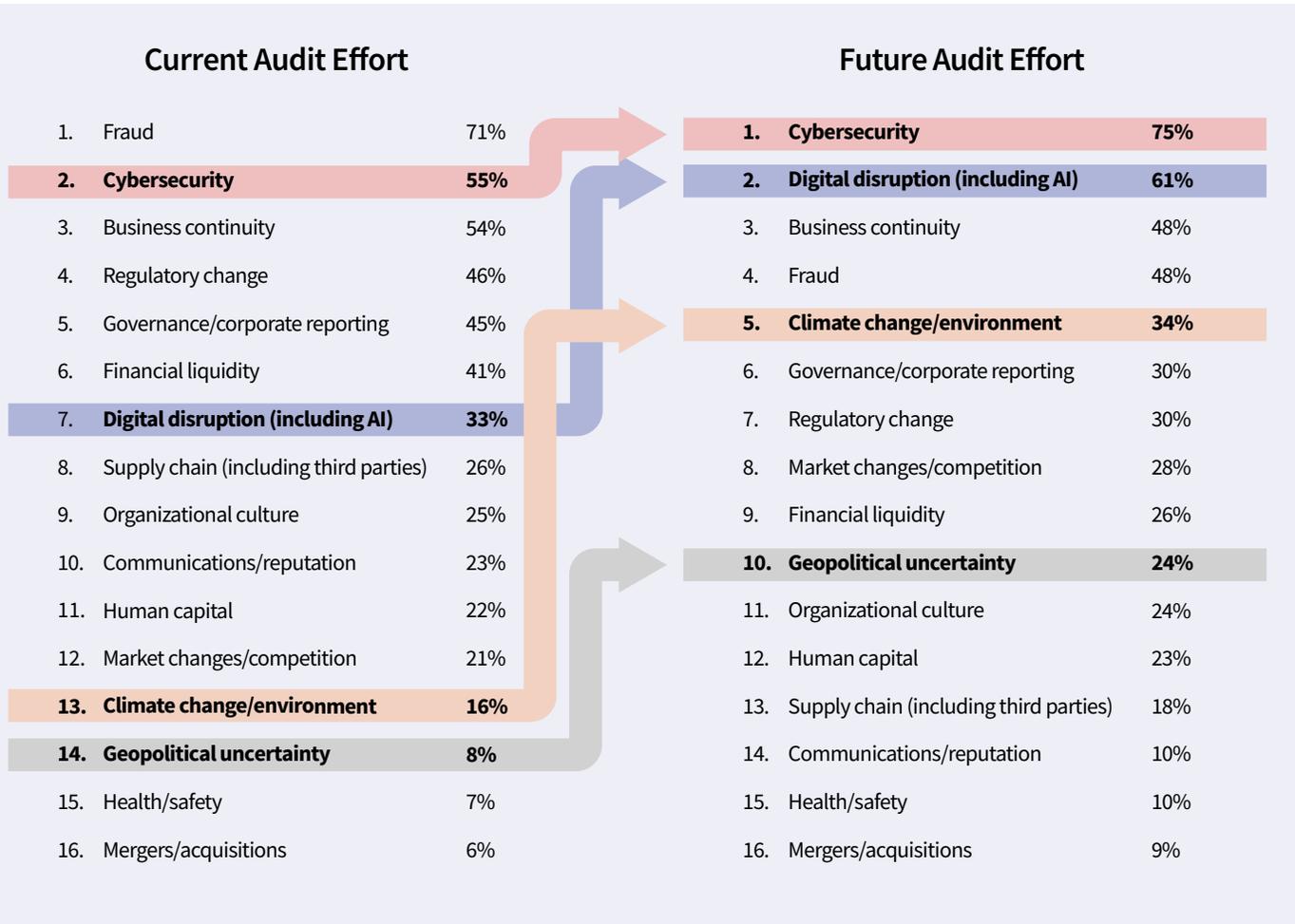
**Most likely, in 2025, CAEs in Indonesia will focus their internal audit efforts in fraud, cybersecurity, business continuity, regulatory change, and governance/corporate reporting.**

**Both Indonesia and Southeast Asia prioritize cybersecurity as a key area for future audit efforts (75% and 76%, respectively). However, Indonesia places greater emphasis on fraud in current efforts (71% vs. 50% in Southeast Asia), while Southeast Asia is more focused on cybersecurity, business continuity, and governance/corporate reporting. Looking ahead, both regions show increasing attention to climate change, but Indonesia lags slightly in prioritizing digital disruption and business continuity compared to Southeast Asia.**



# INDONESIA – RISK TRENDS

## Expected Audit Effort Change In 3 Years – Indonesia



**In the next 3 years, cybersecurity risk is expected to be the most exhaustive effort in internal audit activities.**

**Besides cybersecurity, digital disruption, climate change, and geopolitical uncertainty are also expected to demand more energy in near future.**



# INDONESIA - RISK IN FOCUS

Indonesia top risks 2025 are: cybersecurity, fraud, business continuity, digital disruption (AI), and regulatory change.

## Cybersecurity in Indonesia

Regarding cybersecurity, Indonesia faces a plethora of threats and challenges including cyber attacks through malware, ransomware, and data breaches. These incidents have become a significant concern for many stakeholders, including businesses, government agencies, and individual users. Although the government has prioritized certain cybersecurity initiatives, there is still a noticeable gap in general public awareness about cybersecurity issues. This gap is compounded by a shortage of skilled cybersecurity professionals and insufficient infrastructure to adequately protect the digital ecosystem.

In 2023, Indonesia's share of businesses experiencing cyber incidents in the Asia Pacific region was 52%, according to Statista. This figure underscores the pervasive nature of cyber threats and the urgent need for effective countermeasures. The National Cyber and Crypto Agency (BSSN) reported that in 2023, sectors such as government administration, financial services, and transportation were the most affected by alleged cyber incidents. These sectors' critical roles in national infrastructure make their vulnerability to cyberattacks particularly concerning.

One of the major challenges in addressing cybersecurity in Indonesia is the lack of public awareness. Many individuals and businesses do not fully understand the importance of cybersecurity practices or the potential consequences of neglecting them. Moreover, the shortage of skilled cybersecurity professionals means that even when organizations recognize the need for improved security, they may struggle to implement effective measures due to a lack of expertise. This situation is further exacerbated by outdated or inadequate infrastructure that cannot support the necessary security protocols.

To improve cybersecurity in Indonesia, a multifaceted approach is necessary. This includes enhancing public/customer awareness through education and outreach programs, increasing investment in cybersecurity infrastructure, and developing a robust pipeline of skilled professionals through targeted training and certification programs. Collaboration between the government, private sector, and educational institutions will be key to creating a resilient digital ecosystem that can withstand the evolving landscape of cyber threats.

Internal audit functions within organizations must equip themselves with sufficient knowledge and experience in cybersecurity to address these challenges effectively. It is crucial for internal auditors to conduct thorough assessments of the adequacy of cybersecurity controls, including data encryption, access controls, and incident response plans. Regular evaluation of employee training programs on cybersecurity awareness is also essential to ensure that all staff members are informed about best practices and emerging threats. The boards need to be well informed about the organization's use and governance of emerging technologies, including AI.



# INDONESIA - RISK IN FOCUS

## Fraud

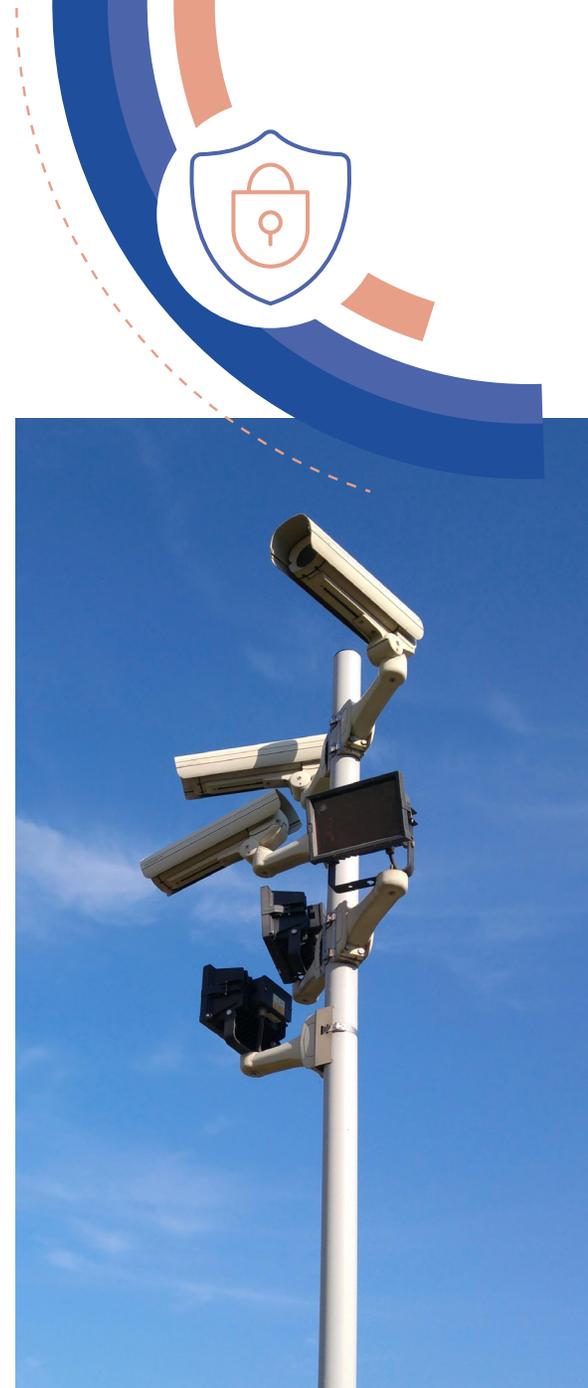
Fraud is a pervasive issue in Indonesia, with some of the most common types including corruption (bribery, embezzlement, and abuse of power to gain profit), manipulation of financial reports, and asset misappropriation. These fraudulent activities can have severe repercussions on businesses and the economy as a whole. Corruption, in particular, erodes public trust and undermines the effectiveness of institutions, making it a significant challenge for both the government and private sector.

The occurrence of fraud can have devastating effects, potentially leading to the downfall of businesses. For instance, the Financial Services Authority (OJK) reported in January 2025 that the majority of Bank Perkreditan Rakyat (BPR) closures were due to weak governance that led to fraudulent activities. When fraud goes unchecked, it not only results in financial losses but also damages the reputation of the organizations involved, leading to a loss of customer confidence and market share.

Addressing fraud in Indonesia requires a multi-faceted approach that includes strengthening governance frameworks, enhancing regulatory oversight, and fostering a culture of integrity. By empowering internal audit functions and equipping them with the necessary tools and resources, organizations can better protect themselves against fraud and ensure long-term sustainability. It is only through collective efforts that the challenges posed by fraud can be effectively mitigated, paving the way for a more resilient and trustworthy business environment.

To enhance fraud prevention measures, organizations should invest in robust internal controls and promote a culture of transparency and accountability. Regular training and awareness programs can help employees recognize and report potential fraud. Moreover, leveraging technology, such as data analytics and forensic tools, can aid in identifying patterns and anomalies that may indicate fraudulent activities. Collaboration between internal audit, management, and other stakeholders is key to creating a comprehensive fraud prevention strategy.

Internal audit plays a crucial role in mitigating the risks associated with fraud. It is essential for internal auditors to conduct thorough fraud risk assessments to identify vulnerabilities within an organization. By investigating suspicious activities and monitoring compliance with anti-corruption regulations, internal auditors can help detect and prevent fraudulent behavior. Additionally, implementing ongoing fraud monitoring systems allows organizations to catch suspicious activities early, before they escalate into significant issues. Board needs to be updated regularly on fraud cases and action taken to deal with the issues.



# INDONESIA - RISK IN FOCUS

## Business Continuity

Natural disasters and pandemics pose significant risks to business operations in Indonesia. The COVID-19 pandemic, in particular, highlighted the importance of having robust business continuity plans in place. The pandemic's impact on global health and economies underscored the need for businesses to be prepared for unexpected disruptions. In addition to pandemics, natural disasters such as earthquakes, floods, landslides, and volcanic eruptions are prevalent in Indonesia, making it imperative for businesses to develop and maintain comprehensive business continuity strategies.

The global economic slowdown and geopolitical uncertainties have created significant headwinds for businesses. Rising inflation, supply chain disruptions, and ongoing conflicts in various parts of the world have negatively impacted global trade and consumer confidence. Indonesian businesses have felt the ripple effects of these global challenges, experiencing disruptions in their operations and facing difficulties in maintaining stable supply chains. The combined effect of these external factors has underscored the need for businesses to adopt resilient and adaptable business continuity plans.

Indonesian businesses also face a confluence of interconnected risks, including cybersecurity threats such as ransomware attacks and data breaches. The integration of digital technologies in business operations has increased the attack surface for cyber threats, making it essential for

organizations to incorporate cybersecurity measures into their business continuity plans. Ensuring that digital assets are protected and that response plans are in place for potential cyber incidents is critical for maintaining operational resilience.

To enhance business resilience, organizations should invest in ongoing training and simulations to test their business continuity plans. Scenario-based exercises can help identify potential weaknesses and improve response strategies. Collaboration with government agencies, industry peers, and emergency management organizations is also crucial for developing a coordinated approach to disaster response. By fostering a culture of preparedness and continuous improvement, businesses can better navigate the uncertainties of the future and minimize the impact of disruptions on their operations.

Internal audit plays a vital role in ensuring the effectiveness of business continuity and disaster recovery plans. By evaluating these plans, internal auditors can identify gaps and weaknesses that may compromise an organization's ability to respond to disruptions. It is essential for internal audit to assess the organization's ability to maintain critical operations during disruptions, including the effectiveness of communication protocols, resource allocation, and recovery procedures. Regular audits and reviews help ensure that business continuity plans are up-to-date and aligned with evolving risks.



# INDONESIA - RISK IN FOCUS

## Climate Change

Since organizations started to report their sustainability, internal audit functions somehow becoming knowledge centers to ensure compliance requirements are fulfilled and risk impacts are mitigated properly.

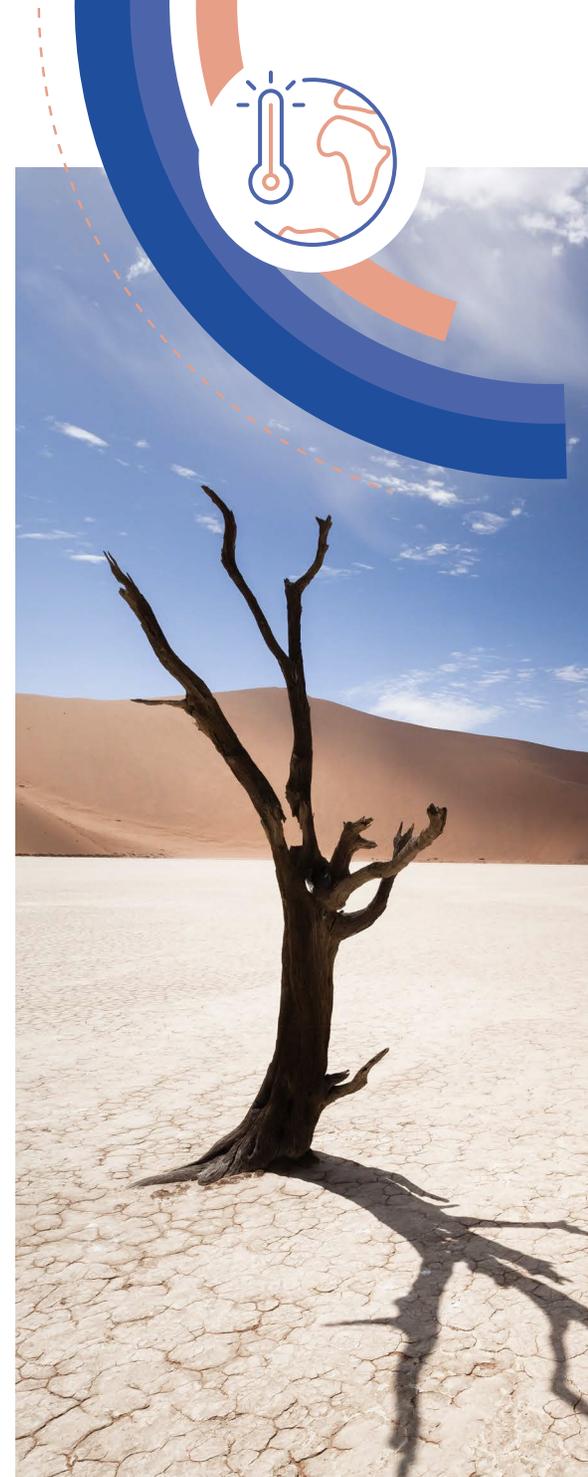
According to report by Central Bureau of Statistics (BPS), challenges faced by Indonesia due to climate change are rising sea levels, more frequent extreme weather events, and deforestation. National Board for Disaster Management (BNPB) claimed that more than 99% disasters in Indonesia are hydro meteorological disaster.

One of the major contributors to climate change in Indonesia is deforestation. This deforestation not only leads to the loss of biodiversity but also contributes significantly to greenhouse gas emissions. Another challenge is the impact of climate change on water resources which affect both the urban and rural population. Drought and water scarcity make agricultural sector vulnerable and resulted in poor harvest performance.

One initiative to combat climate change is that Indonesia is advancing its carbon credits to the global market. Indonesia has set Nationally Determined Contributions (NDCs) to reduce emissions by

915 million tonnes of CO<sub>2</sub> equivalent (MTCO<sub>2</sub>-e) annually by 2030. To achieve this target, Presidential Regulation No. 98 of 2021 establishes a framework for carbon trading and emission reduction, initially focusing on sectors such as forestry and power. Following the regulation, the carbon pricing mechanism is regulated across various sectors and subsectors, each of which has specific ministries coordinating the efforts. While businesses need a comprehensive understanding of these regulations, internal auditors should also be aware of them.

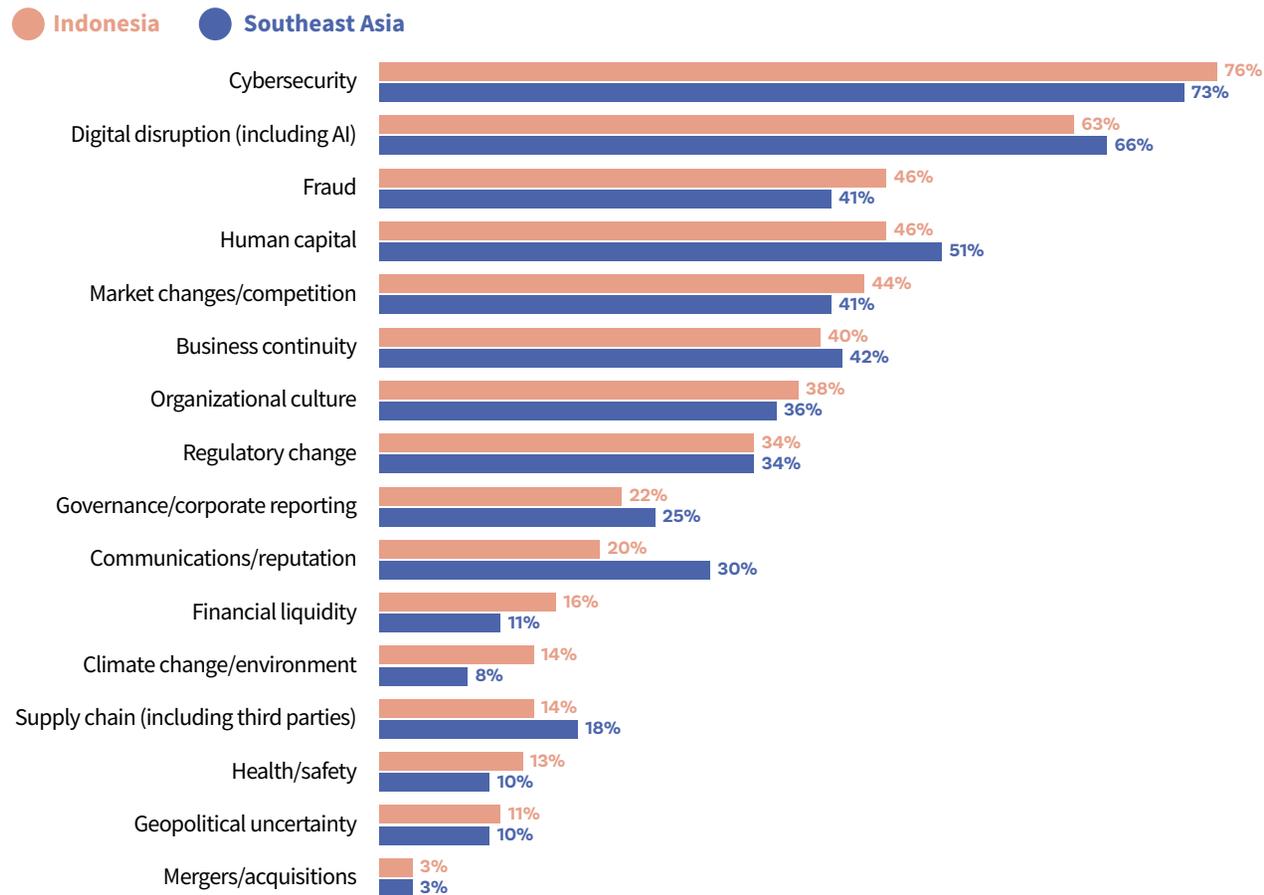
Internal audit and boards play a crucial role in addressing climate change challenges within organizations. They are responsible for ensuring that companies comply with environmental regulations and adopt sustainable practices. Internal auditors conduct risk assessments to identify vulnerabilities related to climate change, evaluate the effectiveness of existing controls, and then monitor compliance with environmental standards and provide recommendations for improvement. Boards, on the other hand, oversee the implementation of these recommendations and ensure that sustainability is integrated into the organization's strategic planning.



# DIGITAL DISRUPTION

## Highest Risk Levels Related to AI - Indonesia

Related to digital disruption, including the usage of AI in different aspects of business processes, internal audit most likely will have to aware on risk of cybersecurity, digital disruption itself, fraud, human capital, and market changes/competition. This situation is similar within Southeast Asian region.



# DIGITAL DISRUPTION

The situation related to digital disruption in Indonesia is almost the same with other south-east asia countries. Some organizations already implemented artificial intelligence, facial recognition, and even blockchain in initial level, although not in organization-wide. In Indonesia, the digital economy is one of the sector that expected to support economic performance growth, as the country do their digital transformation boost by the young demographic that are tech-savvy and better internet penetration rate.

Indonesia has introduced several regulations and road map, such as Digital Indonesia Road Map, National Strategy for Artificial Intelligence (2020-2045). Regulations such as Personal Data Protection Act is designed to protect the privacy and security of individual's personal data and Government Regulation 49 of 2024 regulates the oversight of cryptocurrencies from Commodity Futures Trading Regulatory Agency (Bappebti) to Financial Services Authority.

This digital transformation presents both opportunities and challenges. One of the hardest challenges today is online gambling that become a significant issue where it leads to widespread business disruptions across Indonesia. The pervasive nature of online gambling disguised as harmless game applications already resulted in huge financial losses among users. This affected not only individuals' finances but also disrupts the socio-economic structure. Despite efforts done by government, the challenge persists.

Internal Auditors has a very important and crucial role in ensuring compliance with regulations and ethical standards in the digital disruption landscape. For advisory services, internal audit needs to stay aware and up to date on latest trends in technology, markets, and cybersecurity. Not only that, internal audit also need to support other employees in the organization to stay alert and have routine trainings on cybersecurity and data security.



# INTERNAL AUDIT FOUNDATION PARTNERS

## DIAMOND PARTNERS



## Platinum Partners



## Gold Partners

- Fundación Latinoamericana de Auditores Internos
- IIA–Greece
- IIA–Houston
- IIA–Japan
- IIA–New York
- IIA–Singapore
- Nanjing Audit University

## President's Circle (Individual Donors)

- Larry Harrington, CIA, QIAL, CRMA
- Stacey Schabel, CIA
- Warren W. Stippich, Jr., CIA, CRMA

## Risk in Focus Partners

- |                                      |                      |
|--------------------------------------|----------------------|
| IIA–Argentina                        | IIA–Kenya            |
| IIA–Australia                        | IIA–Malawi           |
| IIA–Bolivia                          | IIA–Mexico           |
| IIA–Botswana                         | IIA–Morocco          |
| IIA–Brazil                           | IIA–Nicaragua        |
| IIA–Canada                           | IIA–Nigeria          |
| IIA–Chile                            | IIA–Panama           |
| IIA–Colombia                         | IIA–Paraguay         |
| IIA–Costa Rica                       | IIA–Peru             |
| IIA–Democratic Republic of the Congo | IIA–Philippines      |
| IIA–Dominican Republic               | IIA–Rwanda           |
| IIA–Ecuador                          | IIA–Singapore        |
| IIA–El Salvador                      | IIA–South Africa     |
| IIA–Gabon                            | IIA–Taiwan (Chinese) |
| IIA–Ghana                            | IIA–Tanzania         |
| IIA–Guatemala                        | IIA–Uganda           |
| IIA–Hong Kong, China                 | IIA–Uruguay          |
| IIA–Indonesia                        | IIA–Venezuela        |
| IIA–Japan                            | IIA–Zambia           |
|                                      | IIA–Zimbabwe         |



# ABOUT THE IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 245,000 global members and has awarded more than 200,000 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](https://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](https://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.

Copyright © 2024 by the Internal Audit Foundation. All rights reserved. For permission to republish, please contact [Copyright@theiia.org](mailto:Copyright@theiia.org).



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](https://theiia.org/Foundation)

