Risk in Focus

Understanding the Risks Your Organization Should be Preparing for in 2025

Lindsay N. Patterson, CPA CIA

Internal Audit FOUNDATION

Internal Audit FOUNDATION

Agenda

- The Research
- The Results: Organization Risks
- The Results: Audit Priorities
- Top Risks: What to Know & Action Steps
    - Cybersecurity
    - Human capital
    - Digital disruption (including AI)
    - Regulatory change
    - Business continuity
    - Market changes

The Institute of Internal Auditors

The Research

Internal Audit FOUNDATION

About Global Risk in Focus

Global cooperation produces new insights

01 Practical, data-driven research to help internal auditors and their stakeholders understand today's risk environment and update their audit plans.

02 Survey results, regional roundtables, and interviews reveal key insights from internal audit leaders worldwide.

03 Partnership between Internal Audit Foundation and the European Institutes Research Group (EIRG).

Internal Audit FOUNDATION

Research Methodology

Global participation

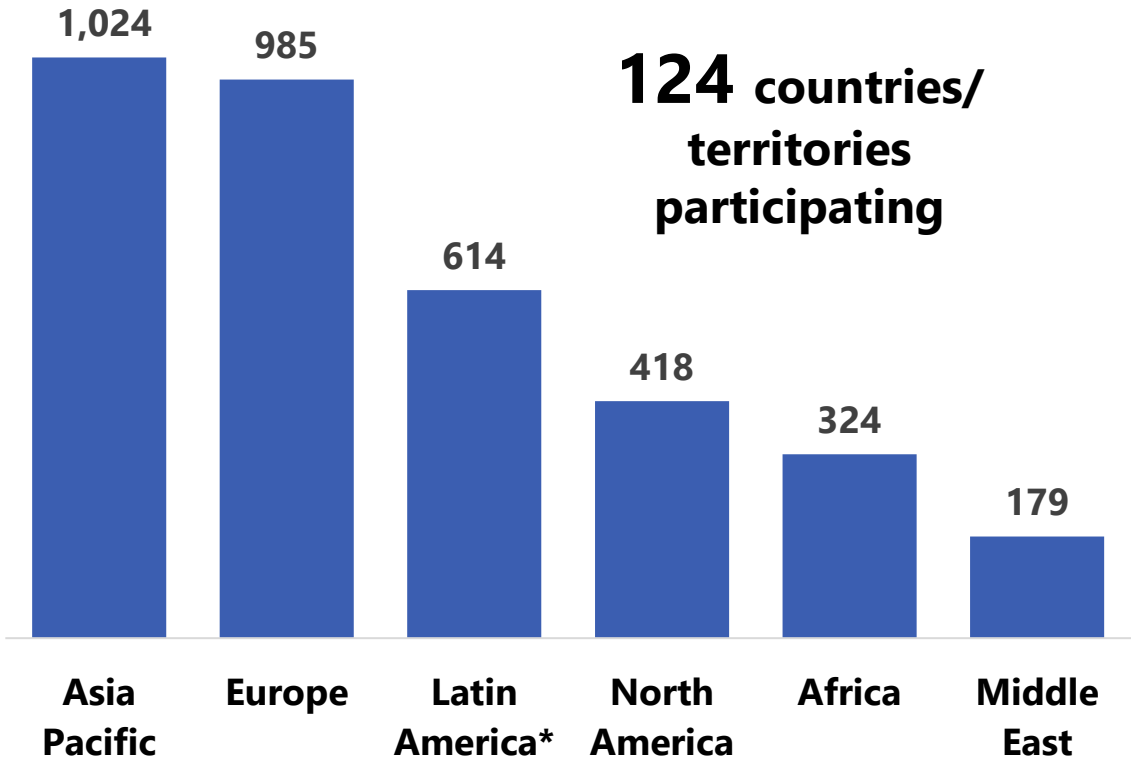
Research Phases

Global survey of internal auditors: 4 March to 20 May 2024

18 roundtables with 138 participants: May 2024

27 in-depth interviews with internal audit experts: June 2024

Survey response total: 3,544



Internal Audit FOUNDATION

Survey approach

16 risk areas were explored

Survey Questions

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

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

The Institute of Internal Auditors

The Results: Organization Risks

Internal Audit FOUNDATION

Global Risk Levels – Region Comparisons

What are the top 5 risks your organization faces?

Analysis

There is broad consensus worldwide about the 4 highest risk areas – cybersecurity, business continuity, human capital, and digital disruption (including AI). However, each region also has some unique areas of concern

5 highest risk areas per industry

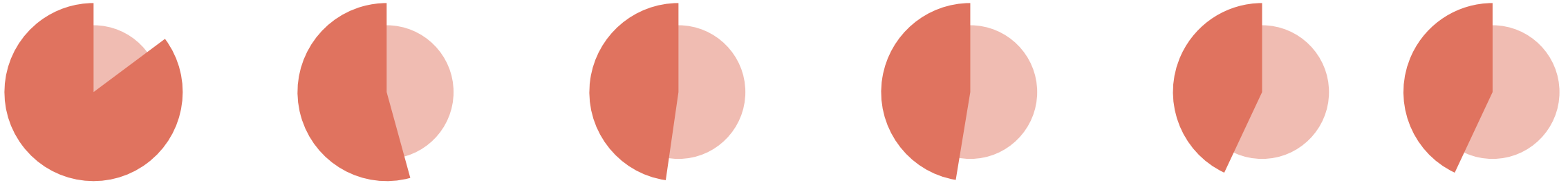
Risk area	Global Average	Africa	Asia Pacific	Europe	Latin America	Middle East	North America
Cybersecurity	73%	64%	64%	83%	74%	66%	88%
Business continuity	51%	57%	62%	32%	49%	63%	41%
Human capital	49%	44%	57%	52%	47%	43%	54%
Digital disruption (including AI)	39%	34%	36%	40%	37%	38%	48%
Regulatory change	38%	32%	32%	46%	45%	27%	47%
Market changes/competition	32%	15%	49%	32%	26%	29%	41%
Financial liquidity	31%	42%	19%	27%	33%	38%	28%
Geopolitical uncertainty	30%	23%	30%	39%	37%	27%	26%
Governance/corporate reporting	25%	31%	22%	20%	18%	41%	16%
Organizational culture	24%	34%	23%	21%	28%	21%	21%
Fraud	24%	42%	22%	14%	32%	27%	9%
Supply chain (including third parties)	23%	16%	24%	29%	17%	26%	29%
Climate change/environment	23%	25%	26%	33%	29%	12%	12%
Communications/reputation	20%	26%	21%	14%	17%	21%	20%
Health/safety	11%	10%	11%	12%	9%	12%	13%
Mergers/acquisitions	6%	4%	4%	8%	4%	8%	8%

If there is a tie for the fifth highest percentage, both percentages are highlighted in a lighter color.

Risk area	Global Average	Africa	Asia Pacific	Europe	Latin America	Middle East	North America
Cybersecurity	73%	64%	64%	83%	74%	66%	88%
Business continuity	51%	57%	62%	32%	49%	63%	41%
Human capital	49%	44%	57%	52%	47%	43%	54%
Digital disruption (including AI)	39%	34%	36%	40%	37%	38%	48%
Regulatory change	38%	32%	32%	46%	45%	27%	47%
Market changes/competition	32%	15%	49%	32%	26%	29%	41%
Financial liquidity	31%	42%	19%	27%	33%	38%	28%
Geopolitical uncertainty	30%	23%	30%	39%	37%	27%	26%
Governance/corporate reporting	25%	31%	22%	20%	18%	41%	16%
Organizational culture	24%	34%	23%	21%	28%	21%	21%
Fraud	24%	42%	22%	14%	32%	27%	9%
Supply chain (including third parties)	23%	16%	24%	29%	17%	26%	29%
Climate change/environment	23%	25%	26%	33%	29%	12%	12%
Communications/reputation	20%	26%	21%	14%	17%	21%	20%
Health/safety	11%	10%	11%	12%	9%	12%	13%
Mergers/acquisitions	6%	4%	4%	8%	4%	8%	8%

Internal Audit FOUNDATION

2025 Top Risks for North American Organizations



88%
Cybersecurity

54%
Human Capital

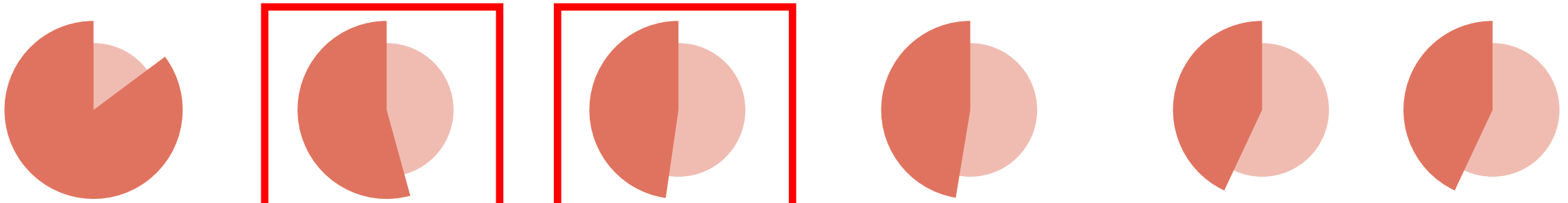
48%
Digital Disruption

47%
Regulatory Change

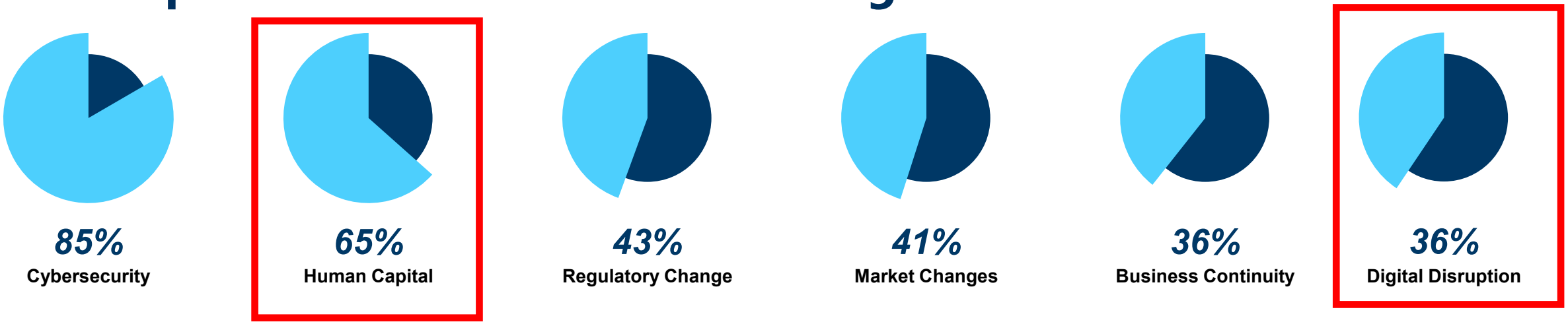
41%
Business Continuity

41%
Market Changes

2025 Top Risks for North American Organizations



2024 Top Risks for North American Organizations



Internal Audit FOUNDATION

North America Risk Levels – Industry Comparison

What are the top 5 risks your organization faces?

Risk area	All	Financial services	Manu-facturing	Public sector	Profes-sional/ technical	Education	Health/ social work	Mining/ energy/ water
Cybersecurity	88%	89%	79%	82%	89%	88%	97%	93%
Human capital	54%	47%	56%	79%	36%	78%	63%	45%
Digital disruption (including AI)	48%	57%	40%	46%	61%	41%	56%	24%
Regulatory change	47%	64%	35%	38%	36%	22%	47%	59%
Business continuity	41%	36%	44%	44%	44%	44%	47%	48%
Market changes/competition	41%	42%	53%	13%	58%	34%	34%	21%
Supply chain (including third parties)	29%	18%	63%	26%	36%	6%	38%	31%
Financial liquidity	28%	44%	21%	13%	19%	38%	22%	14%
Geopolitical uncertainty	26%	23%	42%	18%	28%	16%	9%	28%
Organizational culture	21%	15%	14%	46%	19%	25%	22%	7%
Communications/reputation	20%	16%	5%	38%	19%	44%	13%	17%
Governance/corporate reporting	16%	20%	12%	18%	11%	16%	9%	10%
Health/safety	13%	1%	9%	21%	8%	22%	28%	41%
Climate change	13%	7%	14%	5%	8%	16%	3%	52%
Fraud	9%	15%	0%	13%	11%	13%	3%	0%
Mergers/acquisitions	8%	7%	14%	0%	14%	0%	9%	10%

Analysis

Across most industries, the four areas with highest risk are cybersecurity, human capital, digital disruption, and business continuity. Regulatory change risk is especially high for financial services, driving up the overall average for that area.

5 highest risk areas per industry

Risk area	All	Financial services	Manu-facturing	Public sector	Profes-sional/ technical	Education	Health/ social work	Mining/ energy/ water
Cybersecurity	88%	89%	79%	82%	89%	88%	97%	93%
Human capital	54%	47%	56%	79%	36%	78%	63%	45%
Digital disruption (including AI)	48%	57%	40%	46%	61%	41%	56%	24%
Regulatory change	47%	64%	35%	38%	36%	22%	47%	59%
Business continuity	41%	36%	44%	44%	44%	44%	47%	48%
Market changes/competition	41%	42%	53%	13%	58%	34%	34%	21%
Supply chain (including third parties)	29%	18%	63%	26%	36%	6%	38%	31%
Financial liquidity	28%	44%	21%	13%	19%	38%	22%	14%
Geopolitical uncertainty	26%	23%	42%	18%	28%	16%	9%	28%
Organizational culture	21%	15%	14%	46%	19%	25%	22%	7%
Communications/reputation	20%	16%	5%	38%	19%	44%	13%	17%
Governance/corporate reporting	16%	20%	12%	18%	11%	16%	9%	10%
Health/safety	13%	1%	9%	21%	8%	22%	28%	41%
Climate change	13%	7%	14%	5%	8%	16%	3%	52%
Fraud	9%	15%	0%	13%	11%	13%	3%	0%
Mergers/acquisitions	8%	7%	14%	0%	14%	0%	9%	10%

Risk area	All	Financial services	Manu-facturing	Public sector	Profes-sional/ technical	Education	Health/ social work	Mining/ energy/ water
Cybersecurity	88%	89%	79%	82%	89%	88%	97%	93%
Human capital	54%	47%	56%	79%	36%	78%	63%	45%
Digital disruption (including AI)	48%	57%	40%	46%	61%	41%	56%	24%
Regulatory change	47%	64%	35%	38%	36%	22%	47%	59%
Business continuity	41%	36%	44%	44%	44%	44%	47%	48%
Market changes/competition	41%	42%	53%	13%	58%	34%	34%	21%
Supply chain (including third parties)	29%	18%	63%	26%	36%	6%	38%	31%
Financial liquidity	28%	44%	21%	13%	19%	38%	22%	14%
Geopolitical uncertainty	26%	23%	42%	18%	28%	16%	9%	28%
Organizational culture	21%	15%	14%	46%	19%	25%	22%	7%
Communications/reputation	20%	16%	5%	38%	19%	44%	13%	17%
Governance/corporate reporting	16%	20%	12%	18%	11%	16%	9%	10%
Health/safety	13%	1%	9%	21%	8%	22%	28%	41%
Climate change	13%	7%	14%	5%	8%	16%	3%	52%
Fraud	9%	15%	0%	13%	11%	13%	3%	0%
Mergers/acquisitions	8%	7%	14%	0%	14%	0%	9%	10%

Risk area	All	Financial services	Manu-facturing	Public sector	Profes-sional/ technical	Education	Health/ social work	Mining/ energy/ water
Cybersecurity	88%	89%	79%	82%	89%	88%	97%	93%
Human capital	54%	47%	56%	79%	36%	78%	63%	45%
Digital disruption (including AI)	48%	57%	40%	46%	61%	41%	56%	24%
Regulatory change	47%	64%	35%	38%	36%	22%	47%	59%
Business continuity	41%	36%	44%	44%	44%	44%	47%	48%
Market changes/competition	41%	42%	53%	13%	58%	34%	34%	21%
Supply chain (including third parties)	29%	18%	63%	26%	36%	6%	38%	31%
Financial liquidity	28%	44%	21%	13%	19%	38%	22%	14%
Geopolitical uncertainty	26%	23%	42%	18%	28%	16%	9%	28%
Organizational culture	21%	15%	14%	46%	19%	25%	22%	7%
Communications/reputation	20%	16%	5%	38%	19%	44%	13%	17%
Governance/corporate reporting	16%	20%	12%	18%	11%	16%	9%	10%
Health/safety	13%	1%	9%	21%	8%	22%	28%	41%
Climate change	13%	7%	14%	5%	8%	16%	3%	52%
Fraud	9%	15%	0%	13%	11%	13%	3%	0%
Mergers/acquisitions	8%	7%	14%	0%	14%	0%	9%	10%

Risk area	All	Financial services	Manu-facturing	Public sector	Profes-sional/ technical	Education	Health/ social work	Mining/ energy/ water
Cybersecurity	**88%**	**89%**	**79%**	**82%**	**89%**	**88%**	**97%**	**93%**
Human capital	**54%**	**47%**	**56%**	**79%**	**36%**	**78%**	**63%**	**45%**
Digital disruption (including AI)	**48%**	**57%**	40%	**46%**	**61%**	**41%**	**56%**	24%
Regulatory change	**47%**	**64%**	35%	38%	36%	22%	**47%**	**59%**
Business continuity	**41%**	36%	**44%**	**44%**	**44%**	**44%**	**47%**	**48%**
Market changes/competition	**41%**	42%	**53%**	13%	**58%**	34%	34%	21%
Supply chain (including third parties)	**29%**	18%	**63%**	26%	36%	6%	38%	31%
Financial liquidity	**28%**	**44%**	21%	13%	19%	38%	22%	14%
Geopolitical uncertainty	**26%**	23%	42%	18%	28%	16%	9%	28%
Organizational culture	**21%**	15%	14%	**46%**	19%	25%	22%	7%
Communications/reputation	**20%**	16%	5%	38%	19%	**44%**	13%	17%
Governance/corporate reporting	**16%**	20%	12%	18%	11%	16%	9%	10%
Health/safety	**13%**	1%	9%	21%	8%	22%	28%	41%
Climate change	**13%**	7%	14%	5%	8%	16%	3%	**52%**
Fraud	**9%**	15%	0%	13%	11%	13%	3%	0%
Mergers/acquisitions	**8%**	7%	14%	0%	14%	0%	9%	10%

Risk area	All	Financial services	Manu-facturing	Public sector	Profes-sional/ technical	Education	Health/ social work	Mining/ energy/ water
Cybersecurity	**88%**	**89%**	**79%**	**82%**	**89%**	**88%**	**97%**	**93%**
Human capital	**54%**	**47%**	**56%**	**79%**	**36%**	**78%**	**63%**	**45%**
Digital disruption (including AI)	**48%**	**57%**	40%	**46%**	**61%**	**41%**	**56%**	24%
Regulatory change	**47%**	**64%**	35%	38%	36%	22%	**47%**	**59%**
Business continuity	**41%**	36%	**44%**	**44%**	**44%**	**44%**	**47%**	**48%**
Market changes/competition	**41%**	42%	**53%**	13%	**58%**	34%	34%	21%
Supply chain (including third parties)	**29%**	18%	**63%**	26%	36%	6%	38%	31%
Financial liquidity	**28%**	**44%**	21%	13%	19%	38%	22%	14%
Geopolitical uncertainty	**26%**	23%	42%	18%	28%	16%	9%	28%
Organizational culture	**21%**	15%	14%	**46%**	19%	25%	22%	7%
Communications/reputation	**20%**	16%	5%	38%	19%	**44%**	13%	17%
Governance/corporate reporting	**16%**	20%	12%	18%	11%	16%	9%	10%
Health/safety	**13%**	1%	9%	21%	8%	22%	28%	41%
Climate change	**13%**	7%	14%	5%	8%	16%	3%	**52%**
Fraud	**9%**	15%	0%	13%	11%	13%	3%	0%
Mergers/acquisitions	**8%**	7%	14%	0%	14%	0%	9%	10%

Risk area	All	Financial services	Manu-facturing	Public sector	Profes-sional/ technical	Education	Health/ social work	Mining/ energy/ water
Cybersecurity	88%	89%	79%	82%	89%	88%	97%	93%
Human capital	54%	47%	56%	79%	36%	78%	63%	45%
Digital disruption (including AI)	48%	57%	40%	46%	61%	41%	56%	24%
Regulatory change	47%	64%	35%	38%	36%	22%	47%	59%
Business continuity	41%	36%	44%	44%	44%	44%	47%	48%
Market changes/competition	41%	42%	53%	13%	58%	34%	34%	21%
Supply chain (including third parties)	29%	18%	63%	26%	36%	6%	38%	31%
Financial liquidity	28%	44%	21%	13%	19%	38%	22%	14%
Geopolitical uncertainty	26%	23%	42%	18%	28%	16%	9%	28%
Organizational culture	21%	15%	14%	46%	19%	25%	22%	7%
Communications/reputation	20%	16%	5%	38%	19%	44%	13%	17%
Governance/corporate reporting	16%	20%	12%	18%	11%	16%	9%	10%
Health/safety	13%	1%	9%	21%	8%	22%	28%	41%
Climate change	13%	7%	14%	5%	8%	16%	3%	52%
Fraud	9%	15%	0%	13%	11%	13%	3%	0%
Mergers/acquisitions	8%	7%	14%	0%	14%	0%	9%	10%

Risk area	All	Financial services	Manu-facturing	Public sector	Profes-sional/ technical	Education	Health/ social work	Mining/ energy/ water
Cybersecurity	88%	89%	79%	82%	89%	88%	97%	93%
Human capital	54%	47%	56%	79%	36%	78%	63%	45%
Digital disruption (including AI)	48%	57%	40%	46%	61%	41%	56%	24%
Regulatory change	47%	64%	35%	38%	36%	22%	47%	59%
Business continuity	41%	36%	44%	44%	44%	44%	47%	48%
Market changes/competition	41%	42%	53%	13%	58%	34%	34%	21%
Supply chain (including third parties)	29%	18%	63%	26%	36%	6%	38%	31%
Financial liquidity	28%	44%	21%	13%	19%	38%	22%	14%
Geopolitical uncertainty	26%	23%	42%	18%	28%	16%	9%	28%
Organizational culture	21%	15%	14%	46%	19%	25%	22%	7%
Communications/reputation	20%	16%	5%	38%	19%	44%	13%	17%
Governance/corporate reporting	16%	20%	12%	18%	11%	16%	9%	10%
Health/safety	13%	1%	9%	21%	8%	22%	28%	41%
Climate change	13%	7%	14%	5%	8%	16%	3%	52%
Fraud	9%	15%	0%	13%	11%	13%	3%	0%
Mergers/acquisitions	8%	7%	14%	0%	14%	0%	9%	10%

Internal Audit FOUNDATION

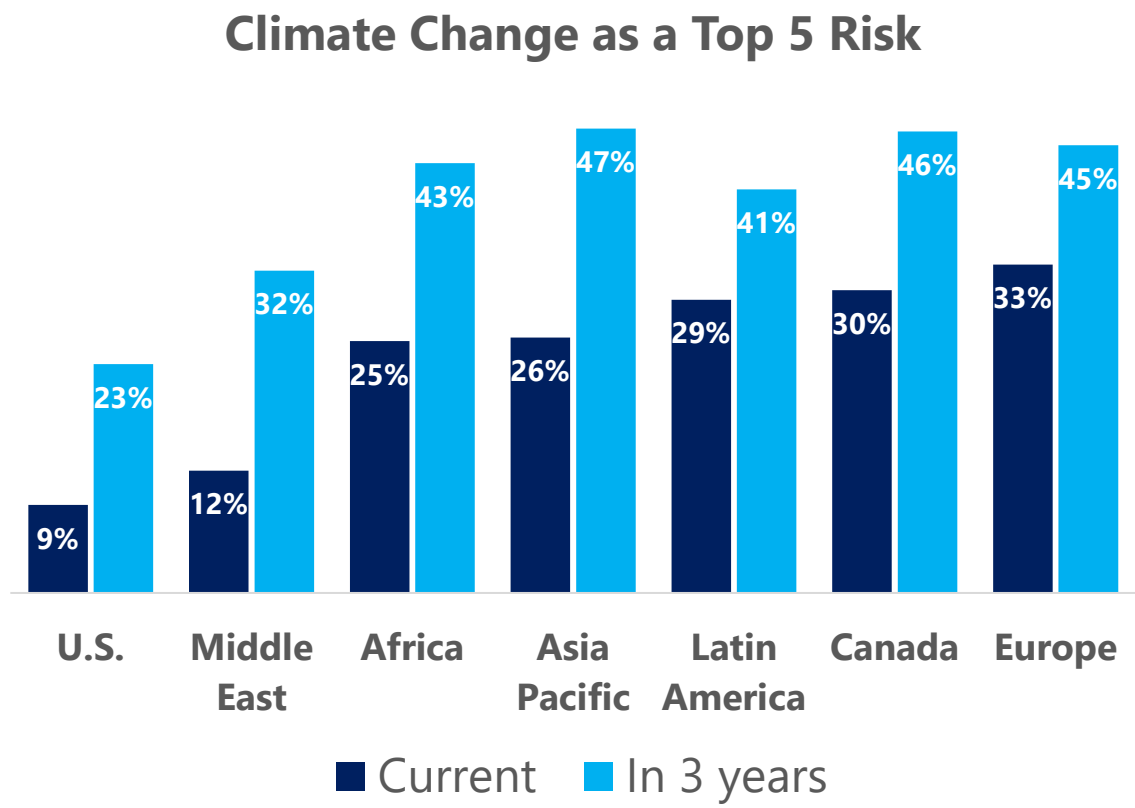
Climate Change Perspectives

Climate change risks are expected to rise in all regions in the next 3 years

01 United States and Middle East currently rate climate change risks significantly lower than other world regions but expect risk to rise rapidly.

02 Internal audit involvement in climate change risks is either driven by regulatory requirements and/or material impacts from extreme weather.

03 Greenwashing is a growing fraud risk in jurisdictions where regulatory requirements are in place and/or customers seek "green" businesses or investments.



Internal Audit FOUNDATION

Risk Drivers for Emerging Risks

Direct pressure and indirect pressure

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

The Institute of Internal Auditors

The Results: Audit Priorities

Internal Audit FOUNDATION

Global Audit Priorities – Region Comparisons

What are the top 5 areas where internal audit spends the most time and effort?

Analysis

69% say cybersecurity is one of the 5 areas where internal audit spends the most time and effort.

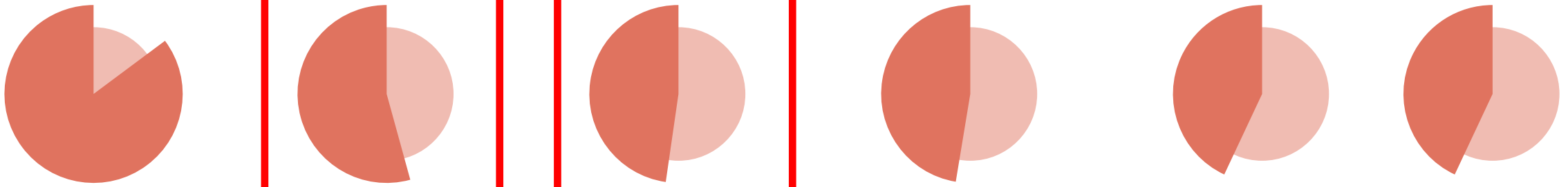
Other top priority areas are governance/corporate reporting (56% of respondents) and business continuity (55% of respondents).

5 highest audit priorities per region

Audit area	Global Average	Africa	Asia Pacific	Latin America	Europe	Middle East	North America
Cybersecurity	69%	56%	63%	67%	74%	65%	87%
Governance/corporate reporting	56%	55%	55%	46%	64%	59%	58%
Business continuity	55%	58%	60%	49%	47%	60%	53%
Regulatory change	46%	39%	52%	47%	51%	35%	54%
Financial liquidity	45%	55%	30%	49%	40%	50%	46%
Fraud	41%	48%	43%	52%	36%	40%	29%
Supply chain (including third parties)	31%	29%	28%	29%	36%	31%	35%
Human capital	31%	36%	33%	29%	28%	35%	27%
Digital disruption (including AI)	25%	24%	23%	19%	23%	31%	33%
Organizational culture	23%	25%	25%	30%	24%	22%	15%
Communications/reputation	20%	24%	23%	22%	14%	18%	17%
Market changes/competition	16%	12%	25%	17%	13%	18%	10%
Health and safety	16%	15%	16%	13%	18%	17%	16%
Climate change/environment	12%	9%	16%	11%	20%	5%	9%
Geopolitical uncertainty	8%	10%	6%	12%	6%	9%	3%
Mergers/acquisitions	6%	4%	2%	7%	7%	7%	10%

Audit area	Global Average	Africa	Asia Pacific	Latin America	Europe	Middle East	North America
Cybersecurity	69%	56%	63%	67%	74%	65%	87%
Governance/corporate reporting	56%	55%	55%	46%	64%	59%	58%
Business continuity	55%	58%	60%	49%	47%	60%	53%
Regulatory change	46%	39%	52%	47%	51%	35%	54%
Financial liquidity	45%	55%	30%	49%	40%	50%	46%
Fraud	41%	48%	43%	52%	36%	40%	29%
Supply chain (including third parties)	31%	29%	28%	29%	36%	31%	35%
Human capital	31%	36%	33%	29%	28%	35%	27%
Digital disruption (including AI)	25%	24%	23%	19%	23%	31%	33%
Organizational culture	23%	25%	25%	30%	24%	22%	15%
Communications/reputation	20%	24%	23%	22%	14%	18%	17%
Market changes/competition	16%	12%	25%	17%	13%	18%	10%
Health and safety	16%	15%	16%	13%	18%	17%	16%
Climate change/environment	12%	9%	16%	11%	20%	5%	9%
Geopolitical uncertainty	8%	10%	6%	12%	6%	9%	3%
Mergers/acquisitions	6%	4%	2%	7%	7%	7%	10%

2025 Top Risks for North American Organizations



88%
Cybersecurity

54%
Human Capital

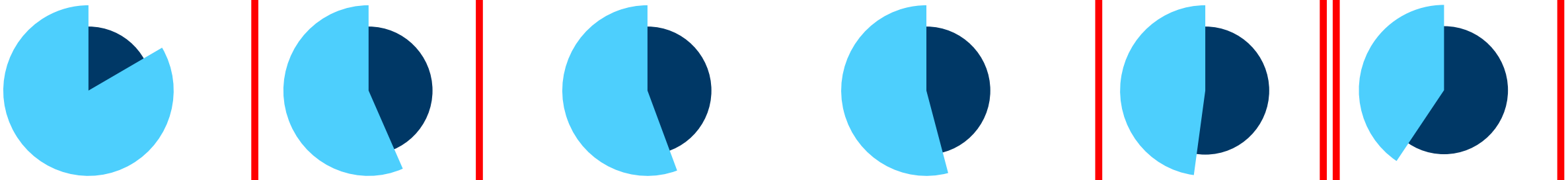
48%
Digital Disruption

47%
Regulatory Change

41%
Business Continuity

41%
Market Changes

2025 Audit Priorities for North American Organizations



87%
Cybersecurity

58%
Governance/ Corporate Reporting

54%
Regulatory Change

53%
Business Continuity

46%
Financial Liquidity

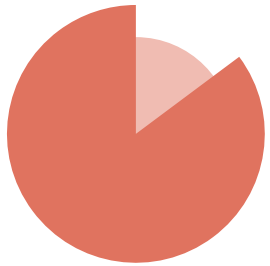
35%
Supply Chain

The Institute of Internal Auditors

Cybersecurity

Cybersecurity

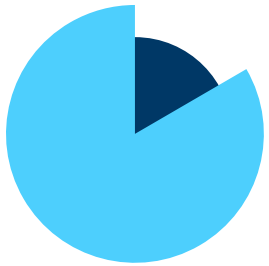
#1 Risk Level



88%

Ranked as Top 5 for Risk Level

#1 Audit Effort



87%

Ranked as Top 5 for Audit Effort

Team building for cyber resilience is key

- New SEC rule adds structure
- Cyber defense requires knowledge
- Collaboration is key to success

Cybersecurity: Action Steps

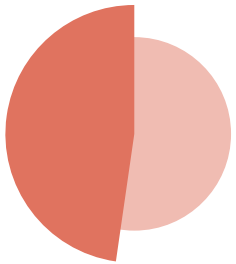
1. Assess the level of awareness to ensure that cyber defense responses are relevant and current.
2. Evaluate the reporting lines between the CISO, the CIO, and the board to ensure risks are communicated and escalated when necessary.
3. Assess faux phishing campaigns and the levels of staff engagement.
4. Educate the board on their governance responsibilities.
5. Evaluate governance processes around shadow IT and whether it is appropriate for the first and second lines to own those technologies.
6. Assess how well the organization’s governance structure enables collaboration across the three lines.

The Institute of Internal Auditors

Human Capital

Human Capital

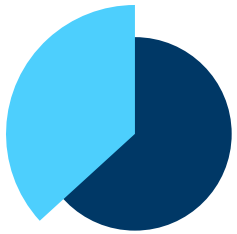
#3 Risk Level



48%

Ranked as a Top 5 for Risk Level

#7 Audit Effort



33%

Ranked as Top 5 for Audit Effort

Negotiating the culture clash

- Diversity is more than skin deep
- Look for non-traditional signs of trouble
- Collaborate to break down siloed recruitment

Human Capital: Action Steps

1. Evaluate management's identification of emerging hybrid working risks and development of effective strategies.
2. Assess corporate cultural practices and communicate them to the board for decision-making.
3. Evaluate the use of diversity metrics in monitoring inclusion policies.
4. Develop strategies to identify cultural problems through personal interactions with audit clients.
5. Evaluate HR framework to attract and retain talent, ensuring clear career progress paths.

The Institute of Internal Auditors

Digital Disruption

Digital Disruption

#3 Risk Level

48%

Ranked as a Top 5 for Risk Level

#7 Audit Effort

33%

Ranked as Top 5 for Audit Effort

Understand how new tech impacts business units

- Most organizations are using AI in some capacity
- AI is directly linked to other major areas of risk
- Proactive conversations are vital

Internal Audit FOUNDATION

77% of businesses globally are using or are exploring the use of AI

Most common uses for AI in business

Customer Service
56%

Digital personal assistants
47%

Inventory management
40%

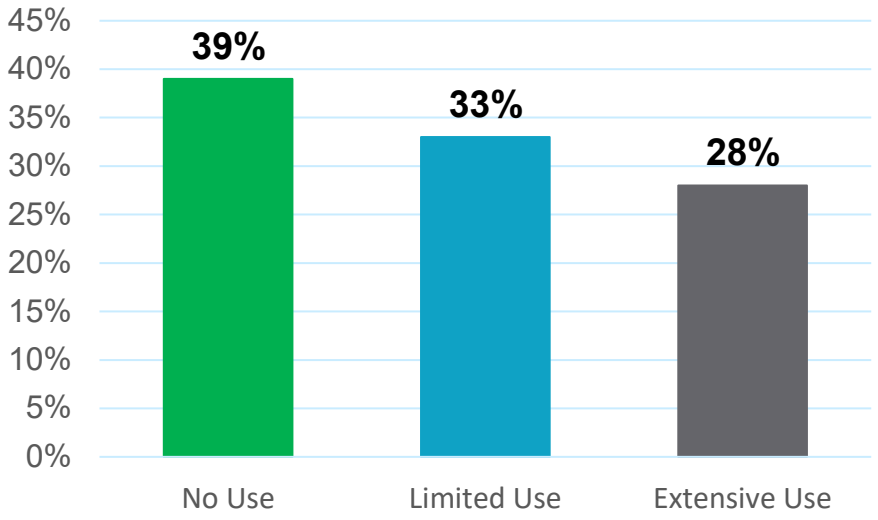
Customer relationship management
46%

Cybersecurity & fraud management
51%

Cybersecurity: Security AI & Automation

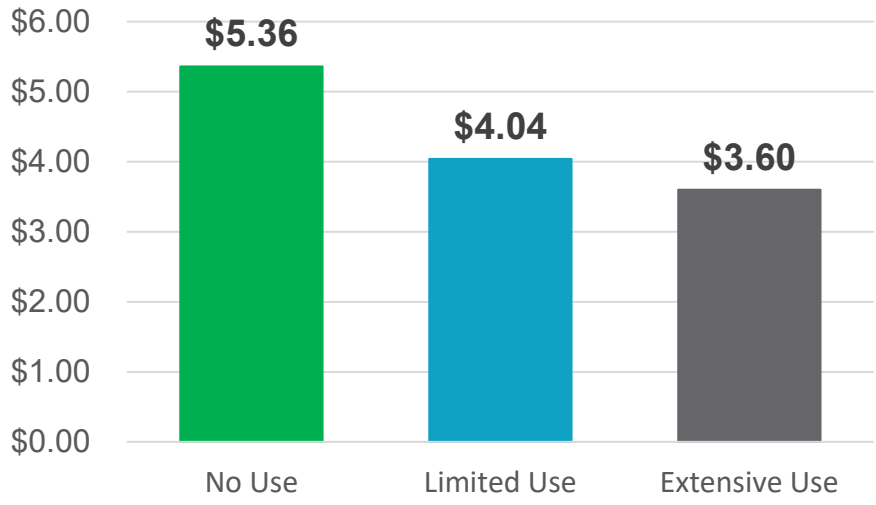
61% **of orgs employ some level of security AI & automation**

State of security AI & automation comparing three usage levels



Percentage of organizations per usage level

Cost of a data breach by security AI and automation usage level



Measured in USD millions

Source: 2023 IBM Cost of Data Report

Internal Audit FOUNDATION

Digital Disruption (including AI) Perspectives

Artificial intelligence (AI) connects to many risk areas

01 The top risks negatively impacted by AI worldwide are cybersecurity, human capital, and fraud.

02 Organizations feel the need to adopt AI to keep pace with competition. As AI is implemented, internal audit provides advisory services to set up processes and controls. After these are in place, internal audit provides assurance.

03 Some internal audit functions are finding ways to test AI and integrate it into internal audit processes. This helps internal audit build AI knowledge needed to provide assurance for their organizations

Digital Disruption: Action Steps

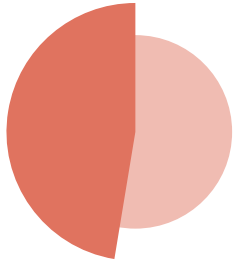
1. Engage with other teams on emerging technologies to provide risk and controls advice on the implementation of new systems.
2. Evaluate how your organization structures and thinks about data, including whether the data taxonomy is granular enough to identify and mitigate appropriate risks.
3. Provide assurance the business identifies core IT systems and processes that can be used to embed privacy and data controls to reduce the compliance burden across the three lines.
4. Proactively broach emerging risks with the board, emphasizing the potential upsides of taking an early-adopter strategic position.

The Institute of Internal Auditors

Regulatory Change

Regulatory Change

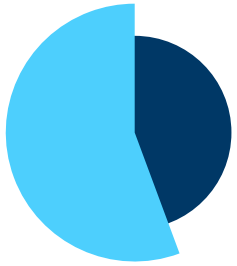
#4 Risk Level



47%

Ranked as a Top 5 for Risk Level

#3 Audit Effort



54%

Ranked as Top 5 for Audit Effort

Staying on top of ever-changing laws and rules

- November could change the focus at the state and federal level
- Data privacy, cybersecurity, and AI regulations are tightening

Regulatory Change: Action Steps

1. Work with legal, compliance, IT, HR, and other teams to develop a comprehensive compliance framework, including regular risk assessments and the updating of policies and procedures.
2. Ensure all departments are aware of and adhere to the latest regulatory requirements. Invest in continuous education and training across the organization.
3. Leverage professional associations and technology to stay on top of changes and manage compliance.
4. Implement scenario planning and stress testing. Model the impact of potential regulatory changes on your organization.
5. Schedule regular internal audits to evaluate the effectiveness of compliance programs.

The Institute of Internal Auditors

Business Continuity

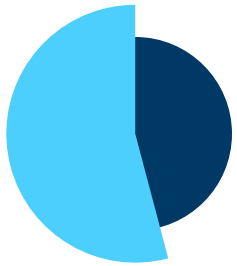
Business Continuity

#5 Risk Level

41%

Ranked as a Top 5 for Risk Level

#4 Audit Effort



53%

Ranked as a Top 5 for Audit Effort

Building resilience in complexity

- Event-based planning is too narrow
- Detailed risk assessments need deeper collaboration
- Planning ahead to fill talent is key

Business Continuity: Action Steps

1. Evaluate the organization’s ERM framework's ability to cover event-based and large-scale disruptive risks.
2. Compare regulatory requirements to establish a suitable strategy for business continuity planning.
3. Help identify second-order or third-order risks that may arise in complex scenarios or due to negative impacts of first-order risk mitigation steps.
4. Ensure a wide range of voices and expertise contributes to brainstorming.
5. Provide an independent voice to evaluate completeness and highlight areas needing additional resources or testing.
6. Ensure resources, personnel, processes, and controls are functional during real-time exercises.

The Institute of Internal Auditors

Market Changes

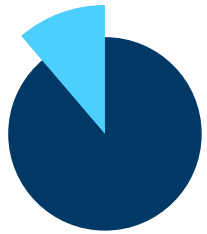
Market Changes

#5 Risk Level

41%

Ranked as a Top 5 for Risk Level

#13 Audit Effort



10%

Ranked as Top 5 for Audit Effort

Adding value with strategic involvement

- Early involvement prevents future problems
- Calculate the costs of market risks
- Bring in experts when needed

Market Changes: Action Steps

1. Evaluate the organization's risk management to track emerging market trends and use them for strategic decision making.
2. Provide input on market-driven technology to ensure risks are assessed and mitigated.
3. Assess how effectively risks from market changes, competition, and consumer behavior are quantified in monetary terms and used in decision-making processes.
4. Assess how well governance processes are responsive to market changes.
5. Evaluate the organization's HR strategies to identify key skills and expertise for future risks.

Internal Audit FOUNDATION

Download Risk in Focus reports at

theiia.org/riskinfocus

New releases 24 Sept. 2024