2025 Audit Committee Survey Insights

Key challenges, concerns, and priorities

KPMG Board Leadership Center

October 2025

Key takeaways

To gain a better understanding of the key challenges, concerns, and priorities impacting audit committee agendas in 2025, the KPMG BLC surveyed 668 audit committee members and chairs as part of a global survey conducted February–May 2025.

Two macro trends—the increased complexity of the business and risk environment, and the geoeconomic landscape—are top of mind.

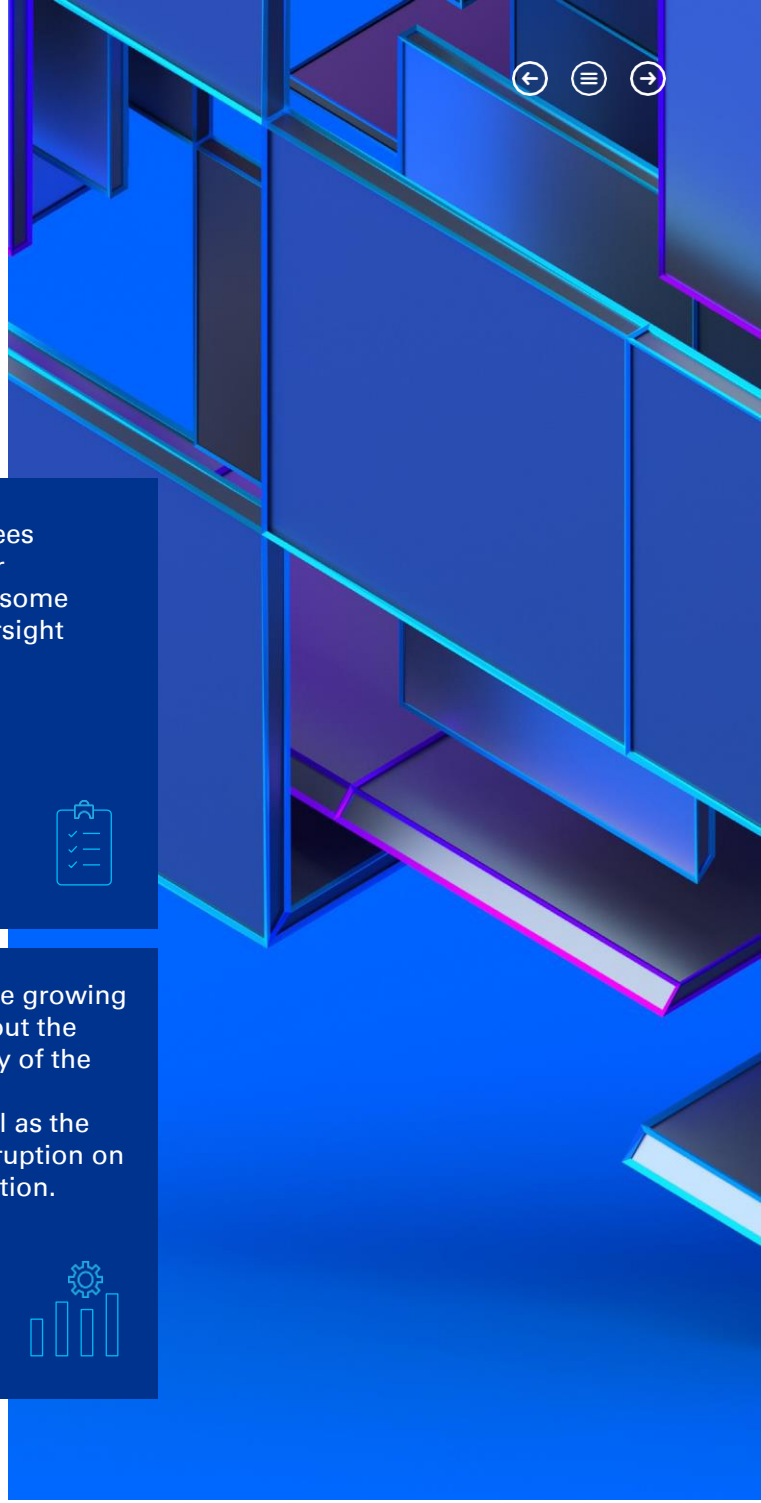
The number of companies with sophisticated risk management—while increasing—is still a minority, and fewer respondents say risk management is keeping pace.

Most audit committees continue to shoulder heavy risk agendas; some are reassessing oversight responsibilities.

Of the risks related to the company's digital activities, cybersecurity and third-party vulnerabilities are viewed as top challenges.

Potential oversight gaps—particularly around cybersecurity, data privacy, and AI—in critical areas of risk are a growing concern.

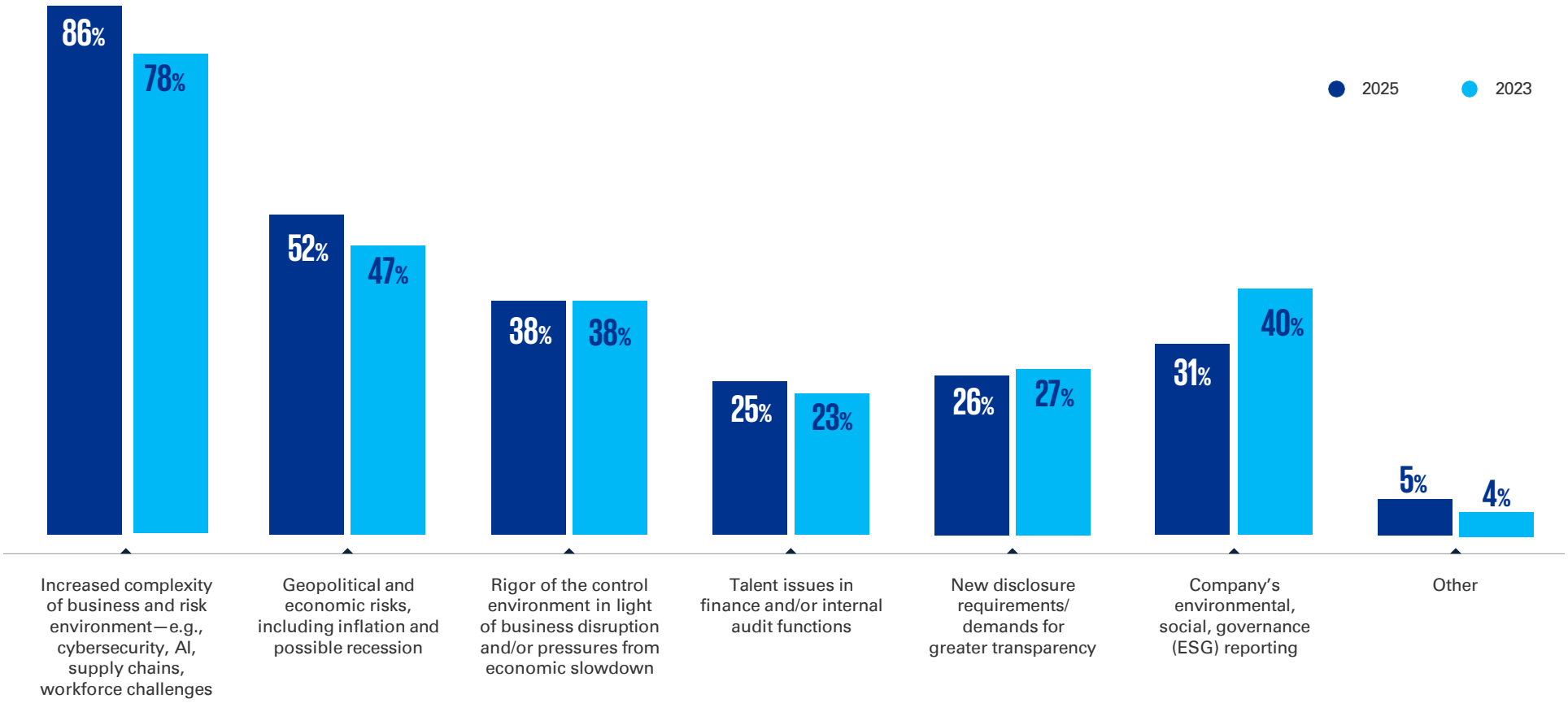
Audit committees are growing more concerned about the increased complexity of the business and risk environment, as well as the impact of digital disruption on the finance organisation.



Two macro trends—the increased complexity of the business and risk environment, and the geoeconomic landscape—are top of mind.

Cybersecurity, AI, supply chain disruptions, and workforce issues, along with geopolitical and economic risks are likely to have the greatest impact on the audit committee's agenda in the coming months. In light of business disruption and the economic slowdown, the rigor of the control environment is also a top concern. Talent issues in the finance and/or internal audit functions are less of a concern for companies.

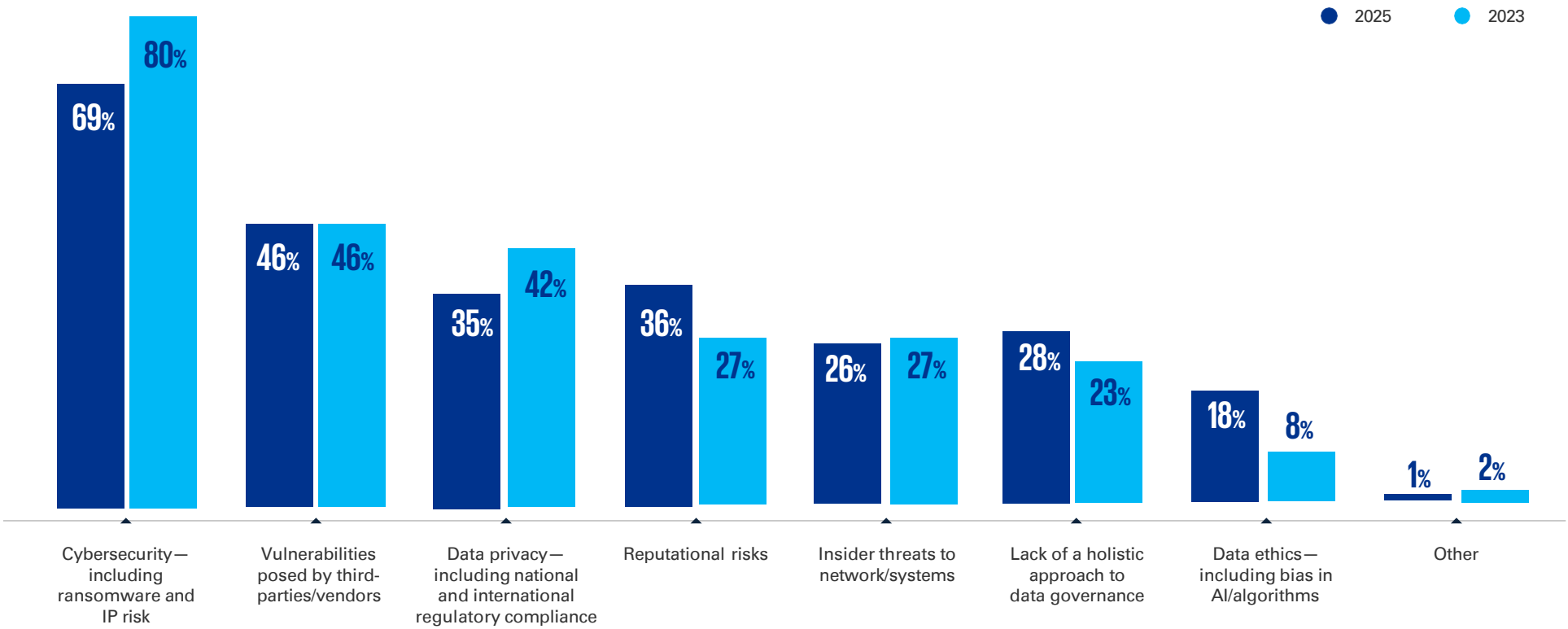
Which macro trends will have the greatest impact on your audit committee's focus and agenda in the months ahead? (select up to 3)



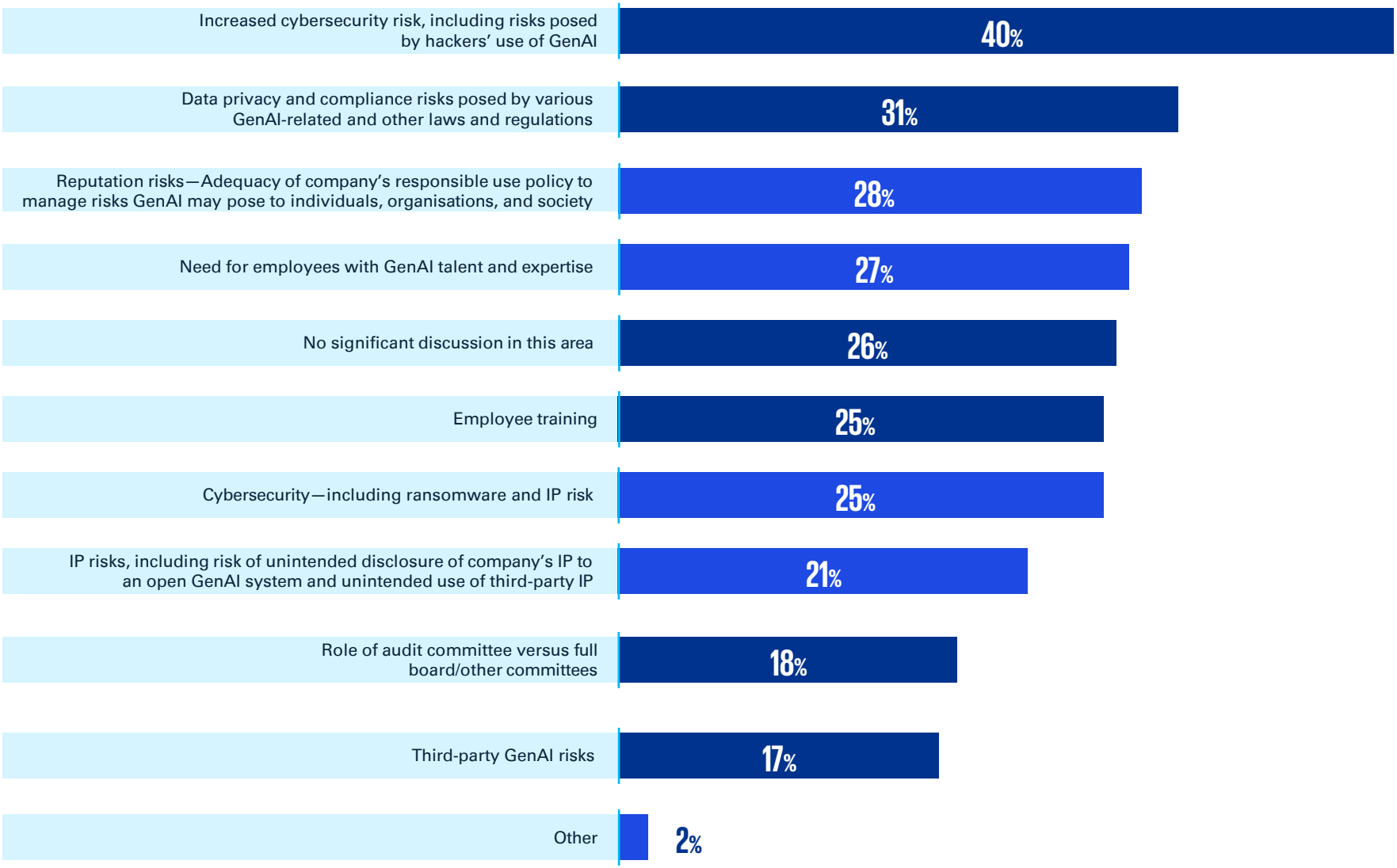
Of the risks related to the company's digital activities, cybersecurity and third-party vulnerabilities are viewed as top challenges.

Ransomware, IP risk, and data privacy (including national and international regulatory compliance) are particularly concerning, as is reputational risk. Cybersecurity and data privacy risks related to the company's use of GenAI, including the need for employee training in AI, are generating significant audit committee discussion. Vulnerabilities posed by third parties/vendors remains as one of the top concerns or challenges of the audit committee. Noteworthy are also the increased concerns or challenges related to reputational risks in 2025 compared to 2023.

Of the risks posed by the company's data/digital activities, which elements are particularly concerning or challenging from the audit committee's oversight perspective? (select up to 3)



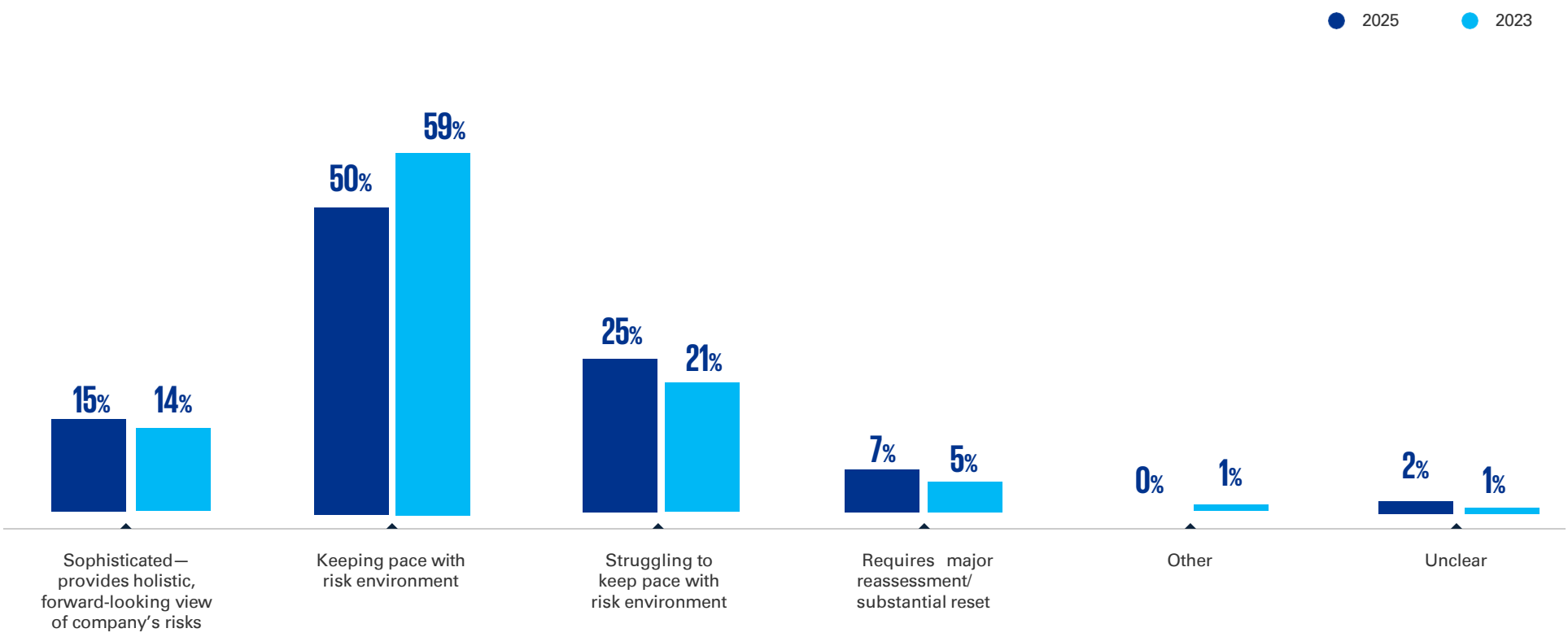
What risks associated with the company's use of GenAI are generating significant discussion in audit committee meetings? (select all that apply)



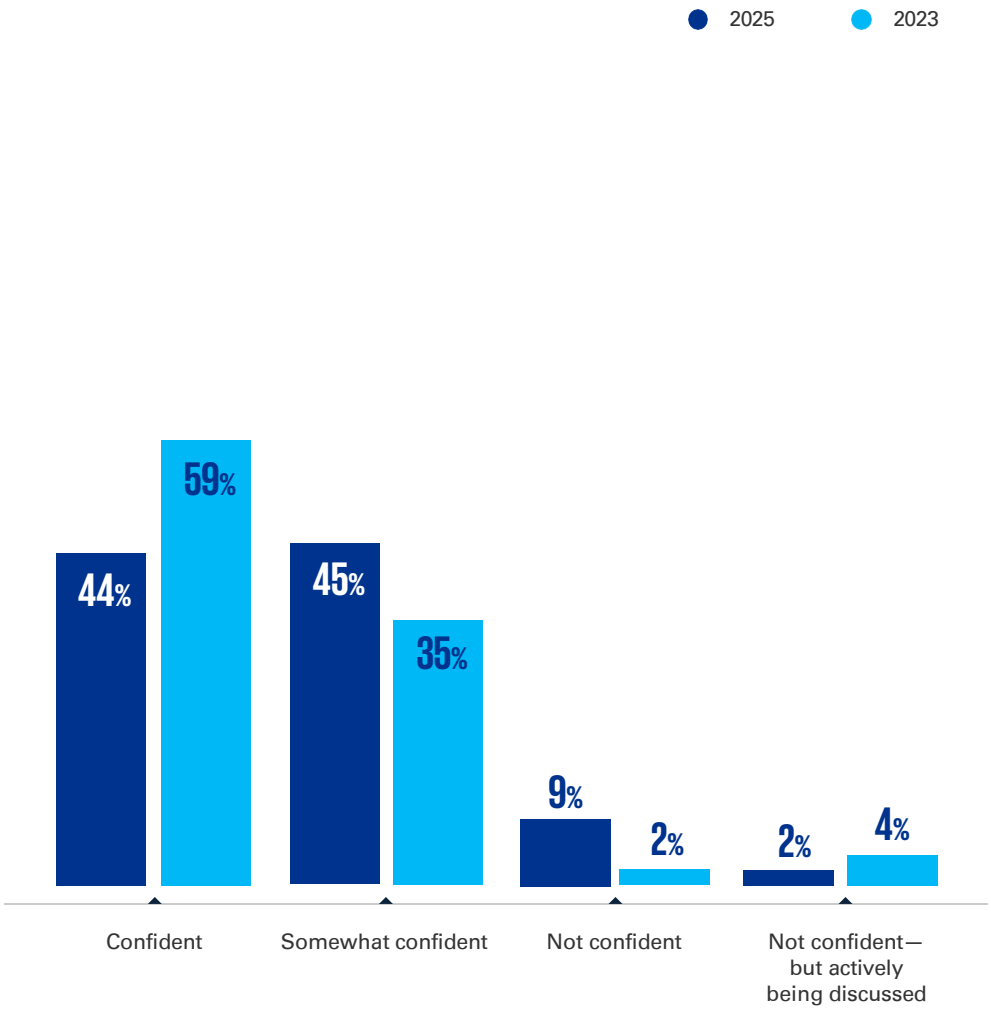
The number of companies with sophisticated risk management—while increasing—is still a minority, and fewer respondents say risk management is keeping pace.

Respondents also express less confidence that there is a clear understanding of the company's mission critical risks by management and the board; that C-suite executives are effectively coordinating and aligning their responsibilities for risk, internal controls, value creation, and related communications and reporting; and that the company is maintaining critical alignments (strategy, risk, culture, controls, incentives).

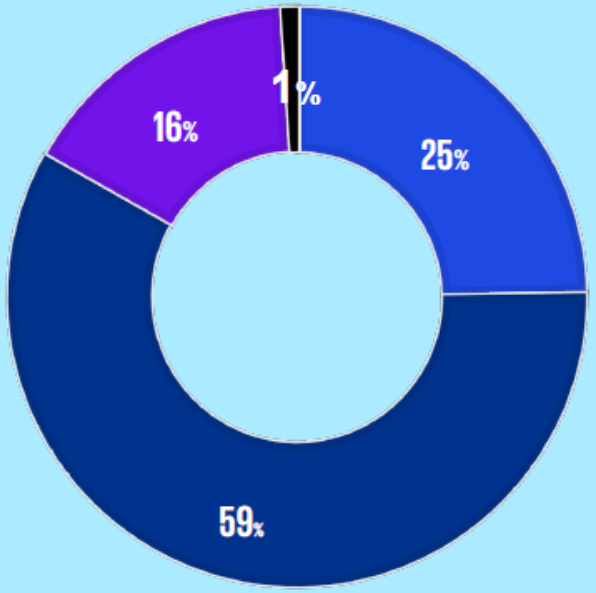
How would you describe the company's risk management and reporting capability? (select one)



How confident are you that there is a clear, common understanding—across the board and management—of what the company's key/mission-critical risks are? (select one)



How concerned are you about the company's ability to maintain critical alignments—culture and purpose, strategy and risk, compliance and controls, incentives, performance metrics, and people—given the disruptions and complexities of the business and risk landscape? (select one)



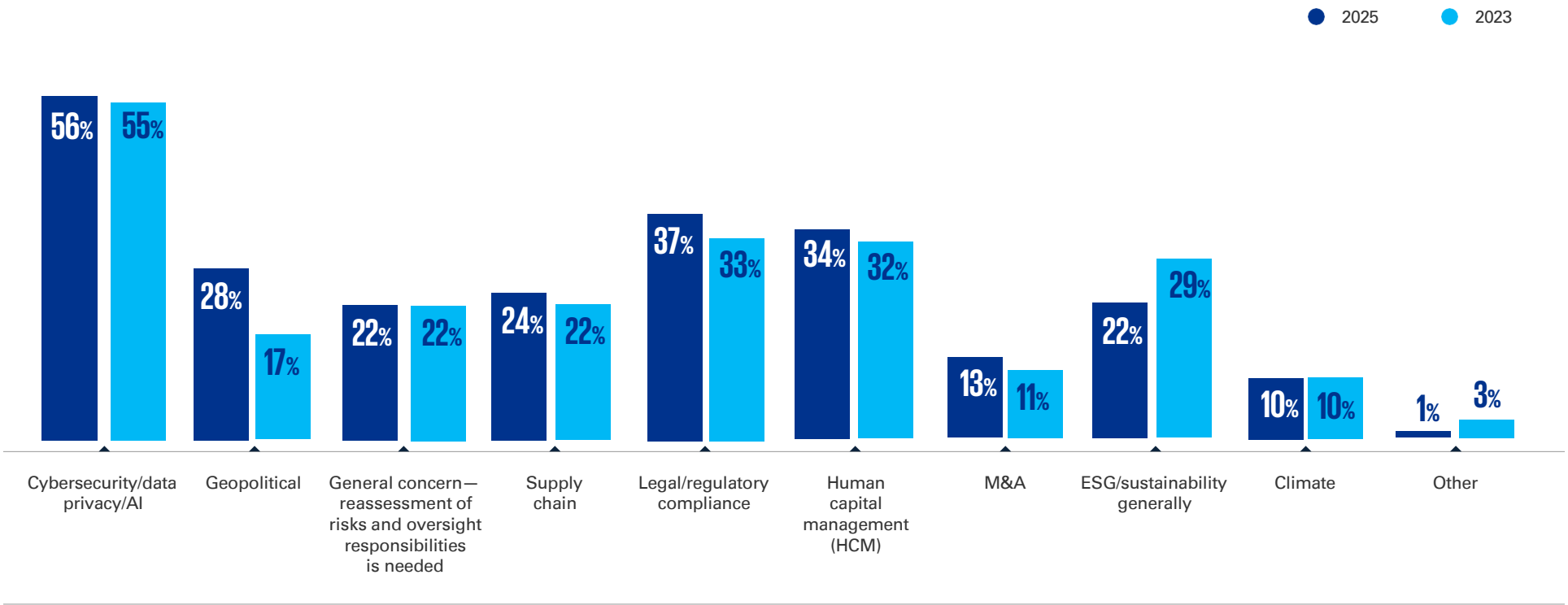
Note: Does not equal 100% due to rounding

Potential oversight gaps—particularly around cybersecurity, data privacy, and AI—in critical areas of risk are a growing concern.

Audit committees are most concerned about potential gaps in board and committee oversight of cybersecurity, data privacy, and AI; legal/ regulatory compliance; human capital management; geopolitical risks; and supply chain risks. Around a quarter of respondents cited the need to reassess board/committee oversight responsibilities for risk.

Given the current geopolitical environment, it is not surprising there is an increased concern about potential oversight gaps by respondents regarding geopolitical risks and risks to supply chains compared to 2023.

Of the various enterprise risks under the purview of multiple board committees, which ones are you most concerned about in terms of potential oversight gaps? (select up to 3)

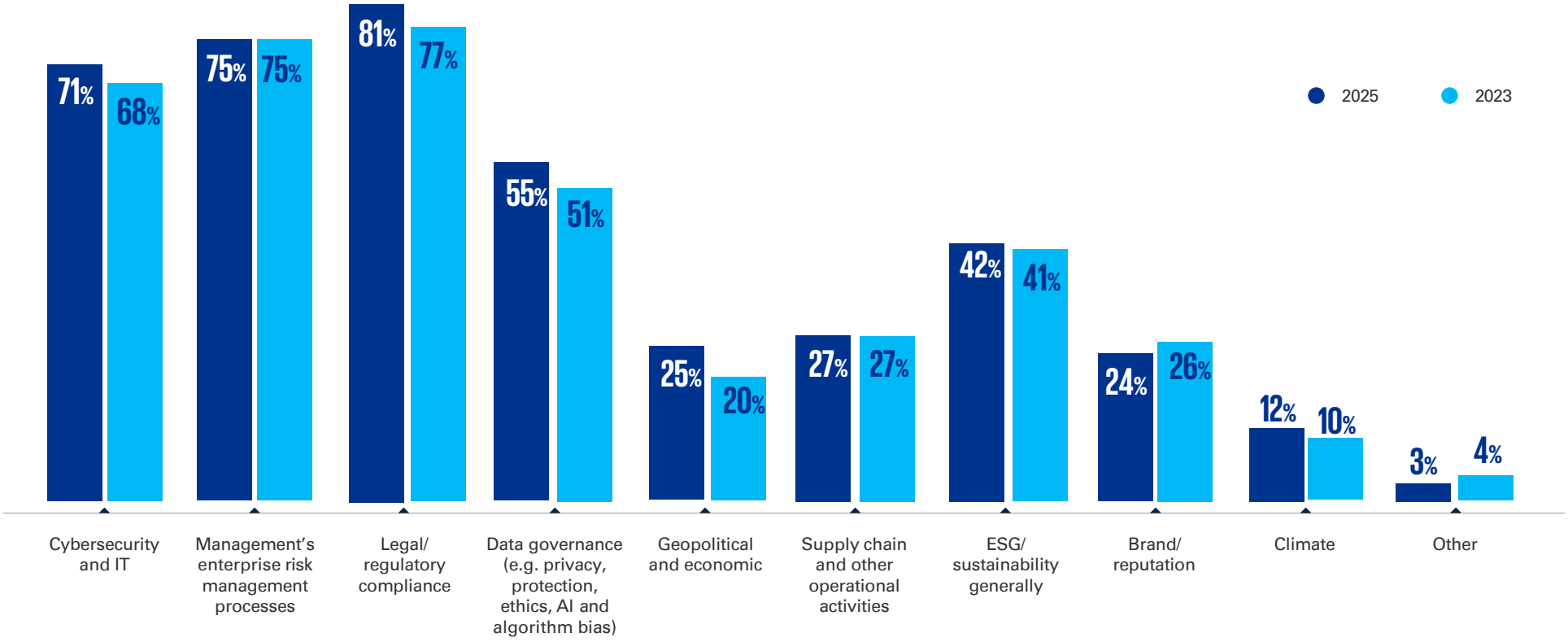


Most audit committees continue to shoulder heavy risk agendas; some are reassessing oversight responsibilities.

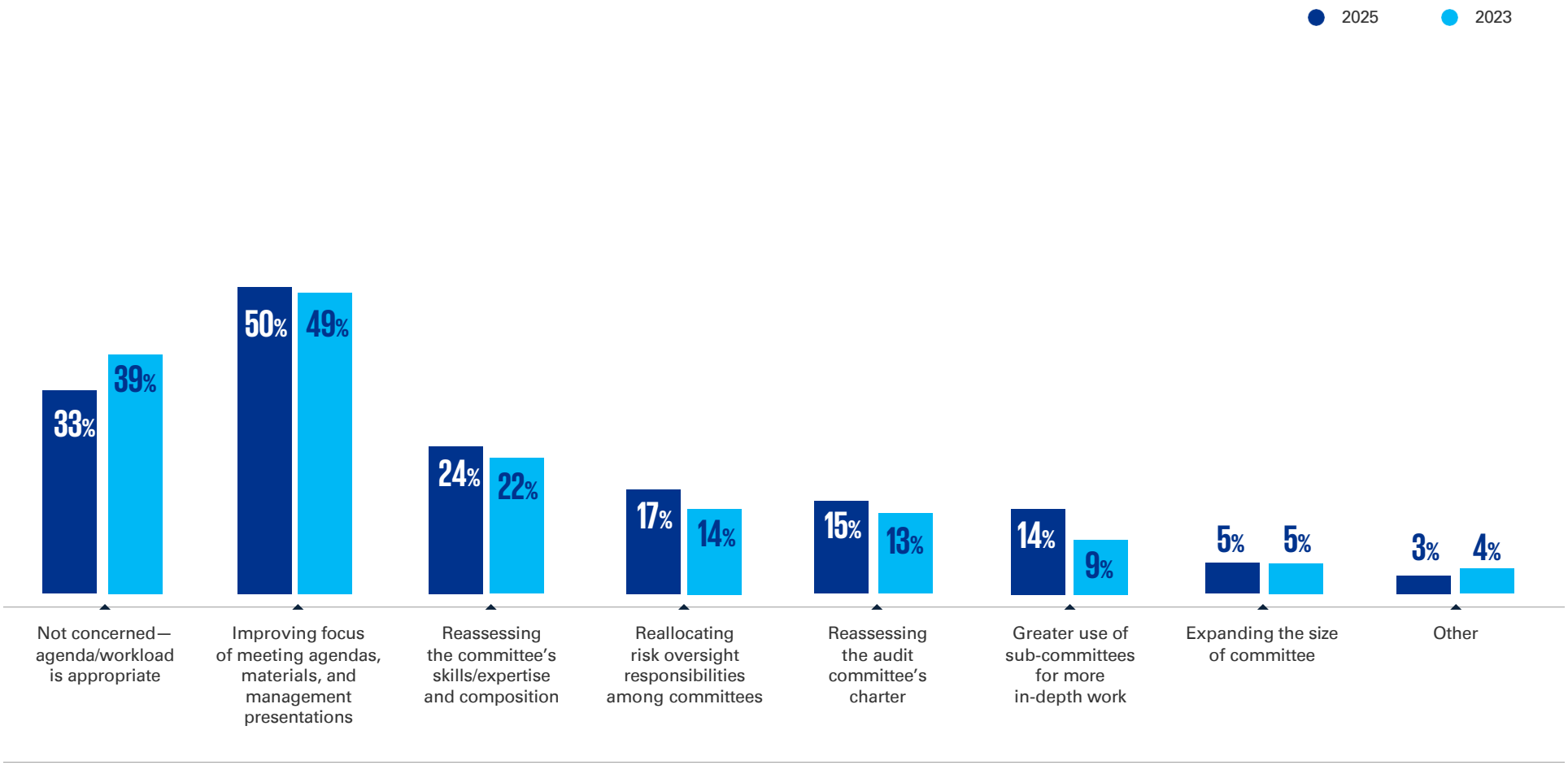
In addition to financial reporting and related control risks, audit committees have significant oversight responsibilities over a broad range of critical risks, including cybersecurity and IT; management's ERM processes; legal/regulatory compliance; and data governance. Some also have significant oversight responsibilities for geopolitical, economic, sustainability, and supply chain risks. Most survey respondents expressed concern about their audit committee's workload, but only 17% said their boards were reallocating risk oversight responsibilities.

Many audit committee members continue to report that their committee has primary oversight over cybersecurity.

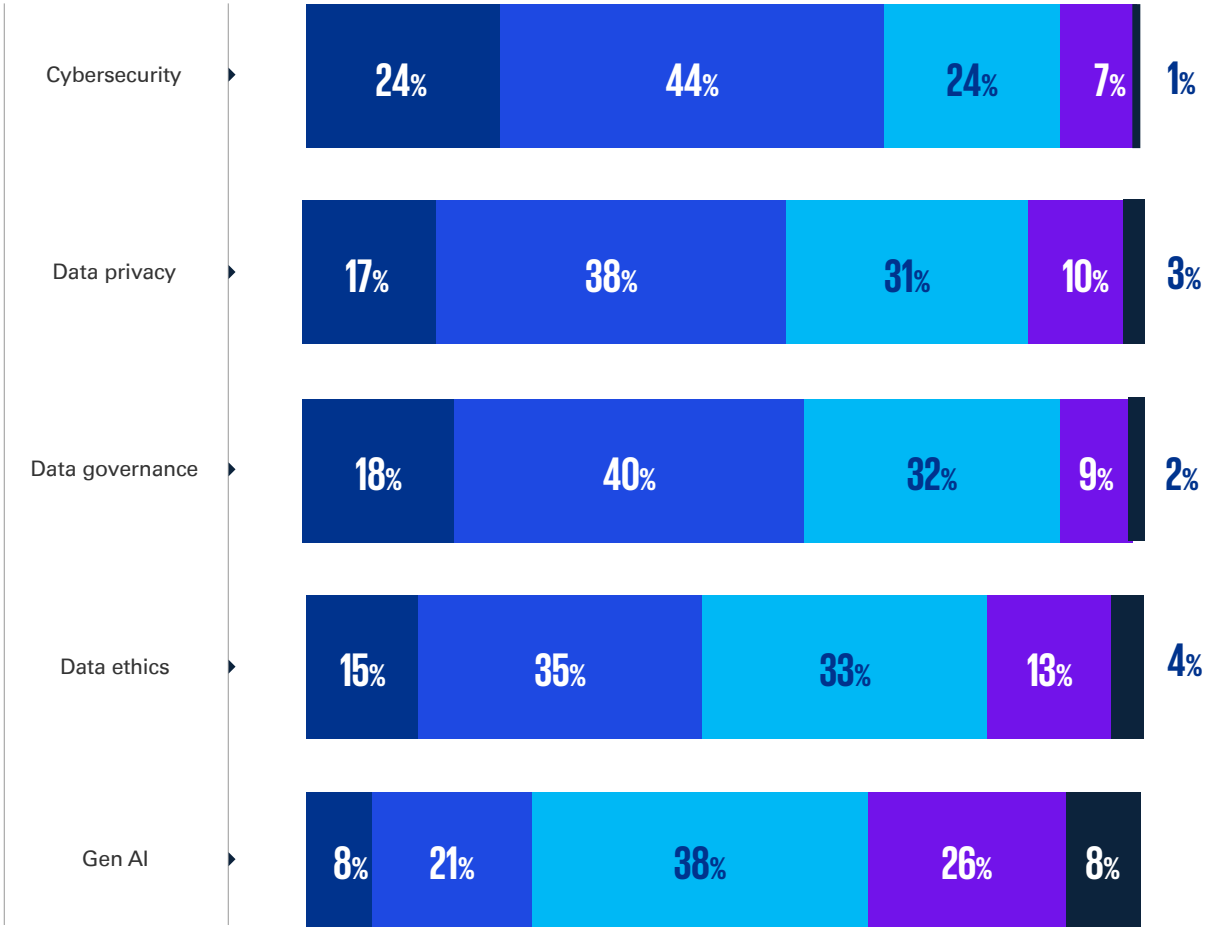
In addition to financial reporting and related control risks, for which risks does your audit committee have significant oversight responsibilities? (select all that apply)



How is your audit committee addressing concerns about the committee's workload? (select all that apply)



What is the scope of the audit committee's oversight responsibility for each of the following areas? (select one per row)

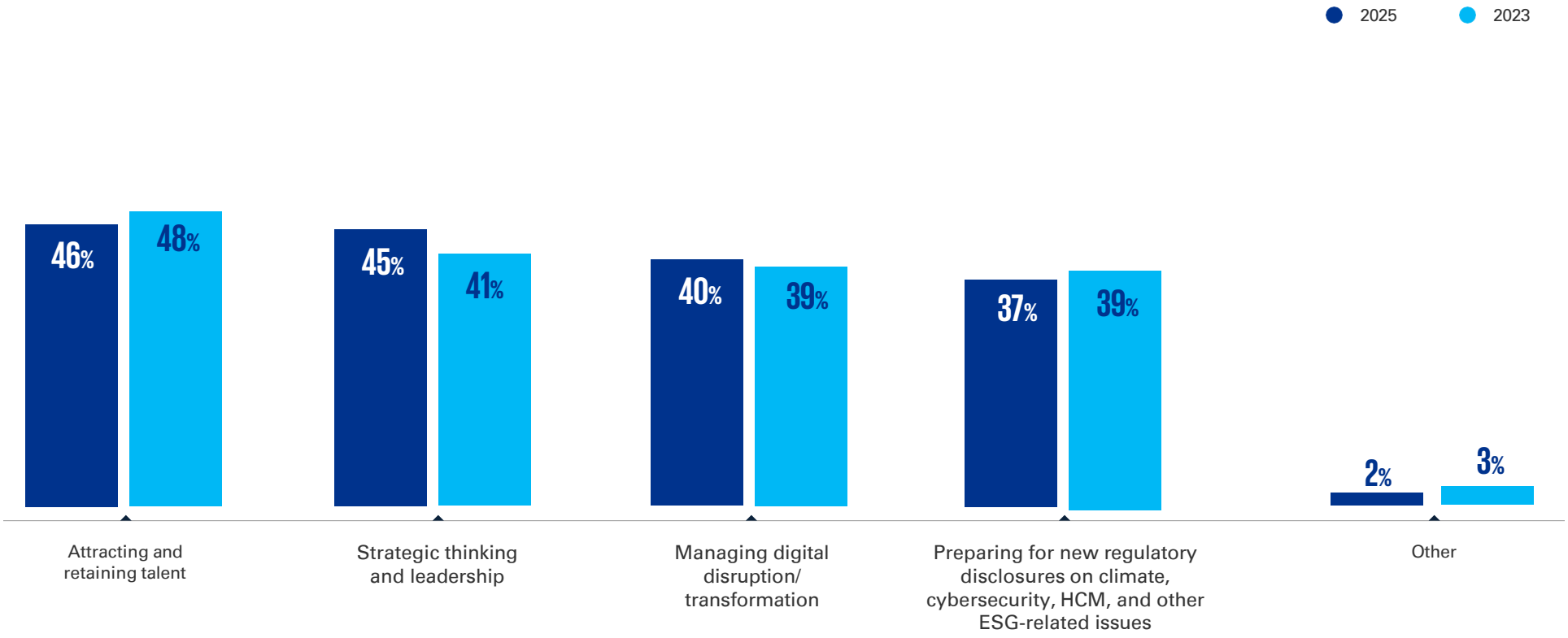


Note: Does not equal 100% due to rounding

Audit committees are growing more concerned about the increased complexity of the business and risk environment, as well as the impact of digital disruption on the finance organisation.

Specific concerns include the finance organisation's ability to attract and retain talent, provide strategic thinking and leadership, and manage digital disruption/transformation.

In your view, what are the top challenges facing the finance organisation? (select up to 2)



Appendix

Country results

This appendix contains detailed data from seven countries that received at least 30 responses. Survey data from all 20 participating countries are included in the global column. Some columns may not total 100% due to rounding.

	Global	Brazil	Colombia	East Africa (Ethiopia, Kenya, Uganda)	Ethiopia	India	Japan	USA
Number of responses	668	92	41	42	31	50	119	85

Which macro trends will have the greatest impact on your audit committee's focus and agenda in the months ahead? (select up to 3)

	%	%	%	%	%	%	%	%
Geopolitical and economic risks, including inflation and possible recession	52	43	66	55	58	48	44	69
Increased complexity of business and risk environment—e.g., cybersecurity, AI, supply chains, workforce challenges	86	84	93	64	55	82	91	88
New disclosure requirements/demands for greater transparency	26	27	15	31	39	46	35	13
Company's environmental, social, governance (ESG) reporting	31	32	22	29	32	26	54	7
Rigor of the control environment in light of business disruption and/or pressures from economic slowdown	38	64	49	29	26	38	20	36
Talent issues in finance and/or internal audit functions	25	23	15	40	42	20	28	25
Other	5	1	5	5	3	4	1	12

In addition to financial reporting and related control risks, for which risks does your audit committee have significant oversight responsibilities? (select all that apply)

	%	%	%	%	%	%	%	%
Cybersecurity and IT	71	84	85	43	42	74	50	75
Climate	12	15	2	5	6	6	12	5
ESG/sustainability generally	42	33	44	26	29	34	54	15
Supply chain and other operational activities	27	17	41	26	23	26	33	15
Geopolitical and economic	25	28	24	36	32	26	23	20
Legal/regulatory compliance	81	84	66	76	77	88	89	73
Data governance (e.g. privacy, protection, ethics, AI and algorithm bias)	55	68	59	45	48	60	40	53
Brand/reputation	24	18	32	19	16	32	34	7
Management's enterprise risk management processes	75	83	63	60	58	62	87	74
Other	3	1	2	0	0	4	2	7

What is the scope of the audit committee's oversight responsibility for each of the following areas? (select one per row)

		%	%	%	%	%	%	%	%
Cybersecurity	Primary oversight	24	23	34	21	23	16	3	46
	Significant oversight	44	54	49	45	48	48	34	27
	Limited oversight	24	21	12	14	13	30	46	19
	No formal oversight	7	2	5	17	13	6	14	8
	Unclear	1	0	0	2	3	0	3	0
Data privacy	Primary oversight	17	12	15	33	39	12	2	34
	Significant oversight	38	55	46	38	35	56	18	24
	Limited oversight	31	29	37	12	10	24	60	27
	No formal oversight	10	3	2	12	13	6	14	14
	Unclear	3	0	0	5	3	2	6	1
Data governance	Primary oversight	18	14	15	29	35	22	2	28
	Significant oversight	40	49	49	38	35	52	25	29
	Limited oversight	32	32	32	24	19	22	59	24
	No formal oversight	9	5	5	7	10	0	10	16
	Unclear	2	0	0	2	0	4	4	2
Data ethics (how the company manages the tension between how it uses customer data in a legally permissible way with customer expectations to protect their personal privacy)	Primary oversight	15	17	22	24	26	16	3	24
	Significant oversight	35	43	51	38	39	40	28	21
	Limited oversight	33	28	22	21	19	34	50	27
	No formal oversight	13	11	2	12	13	6	13	26
	Unclear	4	0	2	5	3	4	6	2
Gen AI	Primary oversight	8	4	15	19	19	8	2	12
	Significant oversight	21	25	34	14	13	12	9	27
	Limited oversight	38	50	29	24	23	44	41	25
	No formal oversight	26	20	15	29	32	30	35	27
	Unclear	8	1	7	14	13	6	13	9

What has been the focus of audit committee discussions regarding cybersecurity? (select up to 3)

	%	%	%	%	%	%	%	%
Increased and more sophisticated cyber threats, including those posed by GenAI	23	27	44	19	10	28	11	28
Need for improvement in company's cyber prevention and detection	47	67	51	48	42	40	58	26
State of company's resilience in event of cyber attack	52	49	37	26	26	54	61	62
Determination of materiality for regulatory filings	10	10	17	17	16	10	2	16
Adequacy of management's cyber incident response plan	45	49	22	24	32	54	50	45
Cybersecurity talent	14	4	22	12	16	10	23	8
Cybersecurity resources / budget	17	12	27	17	19	14	12	18
Third-party cybersecurity risks	26	30	34	17	16	34	13	33
Participation in cyber incident response tabletop exercise	8	15	15	10	10	10	1	6
Role of audit committee versus full board/other committees	17	25	10	17	19	12	5	21
Other	2	0	0	0	0	2	3	5
No significant discussion in this area	5	2	2	19	19	2	10	1

What has been the focus of audit committee discussions regarding data privacy and security? (select up to 3)

	%	%	%	%	%	%	%	%
Compliance with evolving data privacy and security laws and regulations (federal, state, local, and global)	57	67	39	43	42	74	50	47
State of the company's data governance framework, including the controls, processes, and protocols in place around the integrity, protection, availability, and use of the data	64	82	71	43	45	52	51	66
Data ethics	18	25	27	24	26	30	10	12
Need for Chief Data Officer, CISO, CIO, or deeper data talent	14	9	12	10	10	26	14	7
Employee training	32	35	44	33	39	30	47	16
Third-party data governance risks	28	39	32	26	23	38	8	38
Role of audit committee versus full board/other committees	17	23	22	24	26	8	8	25
Other	1	1	0	0	0	0	3	2
No significant discussion in this area	9	1	5	17	16	4	18	7

What is your audit committee's role in the oversight of climate-related issues? (select all that apply)

	%	%	%	%	%	%	%	%
Oversees company's voluntary reporting (quality and disclosure controls)	35	34	34	26	29	42	52	24
Oversees disclosures in regulatory filings	42	43	32	31	26	50	24	55
Oversees management's preparations for US, state, and global disclosures	18	21	0	10	13	10	31	33
Oversees management's disclosure committee activities related to disclosures – including internal controls and disclosure controls and procedures, as well as the committee's composition	39	24	32	31	32	44	63	40

Continued on next page

Continued from previous page

Oversees management's processes to determine which climate risks are material to the business	37	37	41	29	26	46	39	22
Oversees climate-related risks	29	37	39	43	39	26	29	5
Helps to coordinate/allocate oversight responsibilities among board committees	17	21	22	33	39	14	8	12
Other	9	9	12	14	16	8	2	16

Of the various enterprise risks under the purview of multiple board committees, which ones are you most concerned about in terms of potential oversight gaps? (select up to 3)

	%	%	%	%	%	%	%	%
Cybersecurity/data privacy/AI	56	65	56	48	39	64	51	49
Climate	10	11	15	17	13	12	8	4
Human capital management (HCM)	34	34	32	45	45	36	45	19
ESG/sustainability generally	22	16	32	40	45	32	14	5
Legal/regulatory compliance	37	63	37	52	58	38	15	26
Supply chain	24	29	34	2	0	20	34	28
Geopolitical	28	20	29	29	35	32	20	36
M&A	13	12	17	0	0	6	27	16
General concern – reassessment of risks and oversight responsibilities is needed	22	24	32	26	29	30	12	28
Other	1	3	0	0	0	0	1	1

Of the risks posed by the company's data/digital activities, which risks are particularly concerning or challenging from the audit committee's oversight perspective? (select up to 3)

	%	%	%	%	%	%	%	%
Cybersecurity – including ransomware and IP risk	69	65	68	48	42	78	72	71
Insider threats to network/systems	26	23	32	33	39	22	35	19
Data privacy – including national and international regulatory compliance	35	54	27	33	32	50	28	32
Data ethics – including bias in AI/algorithms	18	26	24	24	26	14	17	15
Reputational risks	36	39	56	31	29	36	22	32
Vulnerabilities posed by third parties/vendors	46	49	32	38	32	50	34	62
Lack of a holistic approach to data governance	28	30	29	43	48	24	35	11
Other	1	0	0	0	0	2	2	0

What risks associated with the company's use of GenAI are generating significant discussion in audit committee meetings? (select all that apply)

	%	%	%	%	%	%	%	%
Cybersecurity – including ransomware and IP risk	25	20	22	19	23	26	20	35
Increased cybersecurity risk, including risks posed by hackers' use of GenAI	40	57	54	24	19	34	17	41
Data privacy and compliance risks posed by various GenAI-related and other laws and regulations	31	30	39	21	23	28	24	28

Continued on next page

Continued from previous page

IP risks, including risk of unintended disclosure of company's IP to an open GenAI system and unintended use of third-party IP	21	14	29	21	19	18	19	27
Reputation risks - Adequacy of company's responsible use policy to manage risks GenAI may pose to individuals, organisations, and society	28	39	37	24	26	24	18	20
Need for employees with GenAI talent and expertise	27	22	44	21	23	38	19	22
Employee training	25	26	41	21	29	24	15	22
Role of audit committee versus full board/other committees	18	39	22	21	26	8	3	24
Third-party GenAI risks	17	14	17	17	13	24	4	18
Other	2	3	0	5	0	0	3	2
No significant discussion in this area	26	20	10	33	35	30	48	21

How would you describe the company's risk management and reporting capability? (select one)

	%	%	%	%	%	%	%	%
Sophisticated – provides holistic, forward-looking view of company's risks	15	17	17	7	3	10	4	26
Keeping pace with risk environment	50	49	37	33	32	66	41	58
Struggling to keep pace with risk environment	25	27	34	33	39	10	47	12
Requires major reassessment/substantial reset	7	7	10	24	23	10	3	2
Other	0	0	0	0	0	2	0	0
Unclear	2	0	2	2	3	2	4	2

How confident are you that there is a clear, common understanding – across the board and management—of what the company's key/mission critical risks are? (select one)

	%	%	%	%	%	%	%	%
Confident	44	37	51	29	29	46	27	59
Somewhat confident	45	52	37	57	61	50	42	36
Not confident	9	9	12	5	6	4	28	5
Not confident – but actively being discussed	2	2	0	10	3	0	3	0

How concerned are you about the company's ability to maintain critical alignments—culture and purpose, strategy and risk, compliance and controls, incentives, performance metrics, and people—given the disruptions and complexities of the business and risk landscape? (select one)

	%	%	%	%	%	%	%	%
Very concerned	16	24	10	43	48	24	10	4
Somewhat concerned	59	51	61	45	48	58	71	65
Not concerned	25	24	29	12	3	18	18	32
Other	1	1	0	0	0	0	2	0

In addition to regular interactions/reporting to the board, with whom is the audit committee spending significantly more time in light of the evolving risk & disclosure environment? (select all that apply)

	%	%	%	%	%	%	%	%
Chief accounting officer	37	65	24	29	29	34	28	49
Chief audit executive (CAE)	63	85	59	74	74	42	87	54
Chief risk officer	52	84	54	45	48	50	47	29
Chief sustainability officer	15	13	15	10	10	14	21	2
Chief financial officer	69	79	73	26	29	74	55	81
Chief information security officer	33	48	22	26	35	36	23	39
Chief technology officer	26	49	32	17	23	26	8	38
Chief human resource officer	16	18	17	17	19	18	25	9
General counsel	38	41	51	10	3	22	40	67
Chief tax officer	13	25	20	5	6	6	7	14
Chief compliance officer	41	65	32	19	19	48	49	28
Controller	23	50	15	2	3	16	31	21
Management's disclosure committee	6	7	2	7	10	10	4	4
External auditor	56	70	39	24	29	62	69	56
Other	5	4	7	10	6	8	3	4

How satisfied are you that the company's C-suite executives are effectively coordinating and aligning their responsibilities for risk, internal controls, value creation, and related communications and reporting? (select one)

	%	%	%	%	%	%	%	%
Satisfied	38	34	44	24	26	38	18	62
Somewhat satisfied	50	51	49	69	68	60	56	32
Not satisfied	9	14	5	7	6	2	14	5
Unclear	3	0	2	0	0	0	10	1
Other	0	1	0	0	0	0	2	0

In your view, what are the top challenges facing the finance organisation? (select up to 2)

	%	%	%	%	%	%	%	%
Attracting and retaining talent	46	32	20	36	39	48	77	56
Preparing for new regulatory disclosures on climate, cybersecurity, HCM, and other ESG-related issues	37	57	34	38	39	38	34	9
Managing digital disruption/transformation	40	42	56	36	29	52	17	42
Strategic thinking and leadership	45	28	56	60	68	42	42	53
Other	2	3	2	2	0	2	3	4

How is your audit committee addressing concerns about the committee's workload? (select all that apply)

	%	%	%	%	%	%	%	%
Not concerned – agenda/workload is appropriate	33	20	39	14	13	24	43	44
Reallocating risk oversight responsibilities among committees	17	20	27	19	19	32	7	16
Greater use of sub-committees for more in-depth work	14	5	20	24	19	22	6	8
Expanding the size of committee	5	7	0	5	6	8	2	4
Reassessing the audit committee's charter	15	12	7	33	45	30	4	12
Reassessing the committee's skills/expertise and composition	24	35	20	38	42	26	16	18
Improving focus of meeting agendas, materials, and management presentations	50	75	39	55	55	56	41	41
Other	3	1	0	2	0	0	5	2

What concerns, if any, do you have about your audit committee's composition and skill sets? (select all that apply)

	%	%	%	%	%	%	%	%
No concerns	36	38	41	29	29	32	34	49
Overreliance on the chair or a single member who has deep background /experience to oversee complex financial reporting, disclosures, and control issues	20	17	17	19	19	24	13	21
Lack of expertise in cybersecurity, technology	38	37	20	36	32	58	53	19
Lack of expertise in climate and other ESG issues	24	21	20	33	32	36	30	9
Lack of expertise in risk management	15	16	10	17	19	14	21	13
Committee size – potential need to add members to spread the workload and/or add expertise	15	29	7	7	6	10	9	12
Need for turnover to bring in fresh perspectives	10	14	29	10	10	6	4	5
Lack of diverse views	12	13	10	36	42	12	13	2
Other	1	1	0	0	0	0	4	0

How confident are you that the audit committee currently provides investors, regulators, and other external stakeholders with a robust description of the committee's oversight work? (select one)

	%	%	%	%	%	%	%	%
Confident	46	48	66	29	26	52	22	62
Somewhat confident	43	39	32	57	61	48	48	32
Not confident	8	5	2	7	10	0	27	5
Not confident and currently considering expanding the audit committee report	2	7	0	5	3	0	3	0
Other	1	1	0	2	0	0	1	1

About the KPMG Board Leadership Center

The KPMG Board Leadership Center (BLC) champions outstanding corporate governance to drive long-term value and enhance stakeholder confidence. Through an array of insights, perspectives, and programs, the BLC promotes continuous education and improvement of public and private company governance. BLC engages with directors and business leaders on the critical issues driving board agendas — from strategy, risk, talent, and sustainability to data governance, artificial intelligence, audit quality, proxy trends, and more. Learn more at **kpmg.com/blc**.

Contact Us

Frank Mei

Partner, Head of Governance, Risk and Compliance
KPMG China

T: +86 (10) 8508 7188
E: frank.mei@kpmg.com

Alva Lee

Partner, Head of Governance, Risk and Compliance
Hong Kong
KPMG China

T: +852 2143 8764
E: alva.lee@kpmg.com

Johnson Li

Partner, Governance, Risk and Compliance
KPMG China

T: +86 (10) 8508 5975
E: johnson.li@kpmg.com

Vera Li

Partner, Governance, Risk and Compliance
KPMG China

T: +86 (10) 8508 5870
E: vd.li@kpmg.com