

iapp

C» credo ai

AI Governance Profession Report 2025



Table of contents

What's inside?

Foreword	3
Executive summary.....	5
Part I. Building an AI governance program	10
Case study: AI governance at Mastercard	19
Case study: AI governance at TELUS	21
Case study: AI governance at Boston Consulting Group....	24
Part II. Professionalizing AI governance.....	25
Case study: AI governance at Kroll	32
Case study: AI governance at IBM	34
Part III. Leadership and accountability.....	37
Case study: AI governance at Randstad	40
Case study: AI governance at Cohere.....	49
Conclusion	61
Contacts	63



Foreword

AI governance is not just a compliance exercise.

Artificial intelligence governance can provide businesses with the certainty they need to continue to innovate with AI at scale, building faster, better, more reliable products that are trusted by both consumers and enterprise partners alike.

AI enables global businesses to compete. It makes them faster, more efficient and more competitive. In order to adopt AI confidently, businesses need certainty. The field of work we are in focuses on how to give enterprises the certainty that their AI systems are accountable, trustworthy and safe, removing the barriers to their AI adoption so they can compete with enterprises that are already using AI to win business.

Enterprises have adopted AI, and to stay competitive and continue using it, they now need to manage the risks at scale. Managing AI risk has truly become a reality for enterprises that must ensure compliance with hard regulations that have already come into force, such as the EU AI Act, as well as additional regulations that are already emerging in 2025, such as South Korea's AI Act. The first penalties for noncompliance with AI-specific laws will begin to set a global precedent, forcing businesses to prioritize governance or face steep consequences.

We believe 2025 will mark the year when AI governance becomes a strategic differentiator for companies, and we expect to see real commitments and actions to manage AI risks - learning from both cybersecurity and privacy risk management best practices but incorporating new and unique approaches to AI-specific risks.

Organizations navigating the complexity of AI development and deployment are increasingly considering how AI governance can be an enabling function and success factor for their strategic objectives on AI. Accordingly, how to design and build an AI governance program has fast emerged as a top strategic priority for organizations.

This report charts how the pillars of professionalization – the people, their skills and training, the tools, and processes – are supporting the strategic functions and organizational structures for AI governance. The report dives into the variety of ways in which organizations are approaching, designing, and implementing AI governance, and identifies key and common themes.

One such theme is that it takes a village to build an AI governance program. In addition to an uptick in dedicated AI governance roles being created, communities, committees and cross-functional teams and taskforces are leveraging existing resources and structures as well as taking on the necessary additional and AI governance-specific upskilling and tooling. Privacy, cybersecurity, information technology, ethics, product, marketing, legal and

compliance are just some of the domains and disciplines in the community learning and working together on AI governance.

This burgeoning village of professionals working on AI governance is filling the urgent gap between the demand for experts to implement responsible AI practices and the professionals who are ready to do so. As these practices bed in and scale, organizations are reckoning with the business and strategic benefits of having invested in and prioritized AI governance.

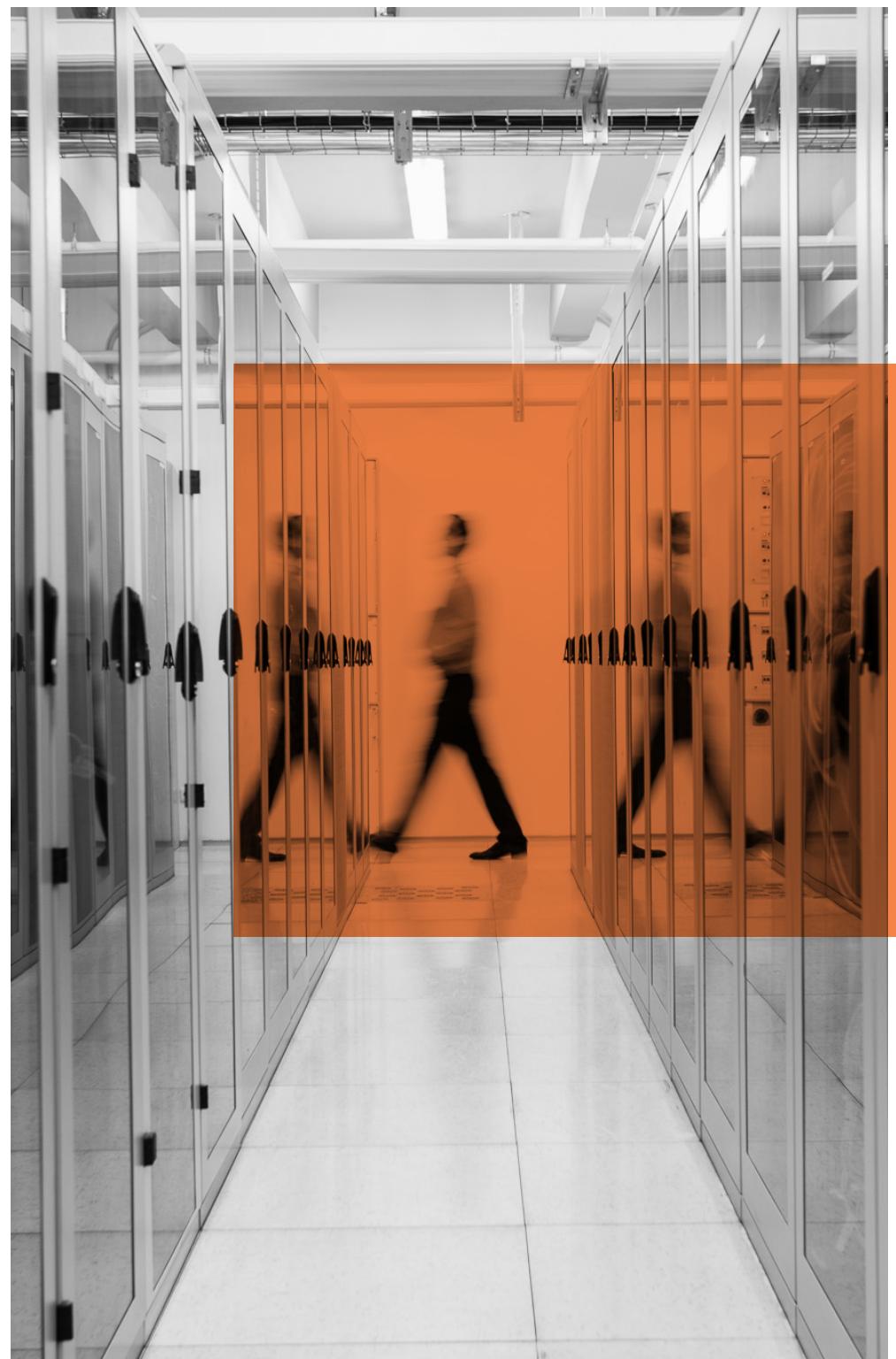
Adopting privacy by design and security by design has always enabled businesses to act faster and be more strategic in the market. Responsible AI by design is no different; it will be essential in an era where businesses that are unable to adopt AI are left behind. Smart investments in secure and robust AI frameworks will allow global companies to move faster and scale better in the longer term.



Joe Jones
IAPP Director of Research
and Insights



Evi Fuelle
Global Policy Director,
Credo AI



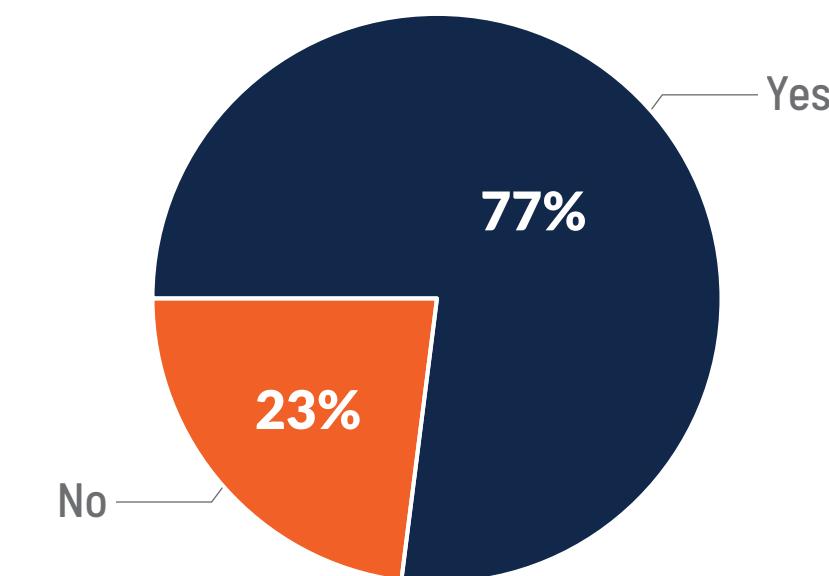
Executive summary

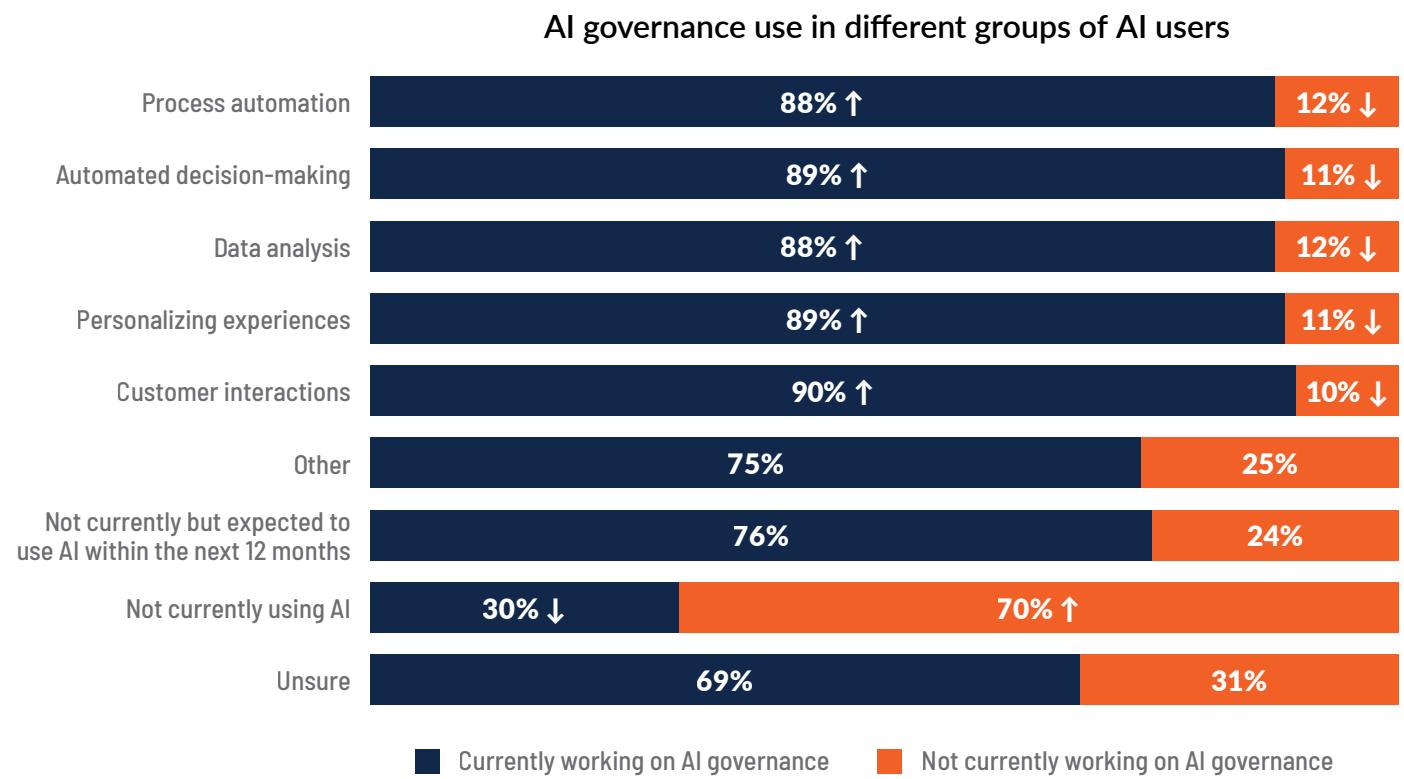
AI governance has proved its value to organizations.

The promulgation of AI governance legislation, regulations and standards combined with increasingly complex and demanding sociotechnical pressures have organizations prioritizing the building and implementation of AI governance programs.

This report, and the data within it, profiles the extent to which organizations are implementing AI governance programs, and how they are doing so. Indeed, survey data shows how the development and deployment of AI by organizations very often goes hand in hand with AI governance.

Is your organization currently working on AI governance?





Of surveyed organizations, 77% are currently working on AI governance, with a jump to near 90% for those organizations already using AI. Importantly, 30% of organizations not yet using AI reported working on AI governance, perhaps revealing a prevailing "governance first" prioritization of ensuring good governance is in place before AI use. This is supported by some of the case studies, which indicate organizations are implementing formal AI governance programs after using AI for smaller use cases but before embracing AI as a strategic imperative.

Starting an AI governance program involves hiring new or dedicating existing employees to an AI governance team. Companies are building these teams incrementally, starting with tasking the existing workforce and then hiring and empowering senior managers and executives, which the data suggests leads to fewer issues using AI and reporting on AI governance, among other positive outcomes. Many of the case studies illustrate how newer AI governance programs hire managers with prior experience in a digital governance discipline, like privacy.

Importantly, 30% of organizations not yet using AI reported working on AI governance, perhaps revealing a prevailing "governance first" prioritization of ensuring good governance is in place before AI use.



**Many organizations with mature
AI governance programs
are drawing in specialists
from several departments,
regardless of the main
AI governance function.**

A significant challenge identified by respondents was access to appropriate AI governance talent and skills in the workforce. Of respondents, 23.5% said finding qualified AI professionals was part of the challenge delivering AI. Another part of the challenge is the host of skills qualified AI governance professionals need. They should, of course, understand AI but also have experience in governance, risk and compliance, and they should be able to translate legislative requirements into actionable policies, for example. While larger companies can split these tasks into several roles, smaller companies will look for AI governance professionals who can cover all these areas. Respondents indicated AI governance skills will continue to evolve alongside the development of new types of AI technologies and policies. Certain skills, such as red teaming, will be increasingly necessary.

There is no clear best practice for how to build and organize an AI governance team, including the location of those directly responsible for AI governance, for example as a separate team or integrated into a broader team responsible for other digital portfolios. From an organizational structure perspective, the data shows 50% of AI governance professionals are typically assigned to ethics, compliance, privacy or legal teams. Many organizations with mature AI governance programs are drawing in specialists from several departments, regardless of the main AI governance function. Over 50% of respondents indicated the following disciplines would gain additional responsibility: privacy, IT, security, and legal and compliance.

Disciplines already involved in digital responsibility are relevant as either the main function or as a collaborating function in AI governance. Organizations often share joint responsibility with privacy and other disciplines, such as cybersecurity or data governance. Respondents indicated AI governance professionals come from different disciplines and areas of expertise, and a strong number of privacy professionals are continually asked to take on AI governance roles.

Organizations building their AI governance programs out of or in conjunction with their privacy programs are likely to adapt those structures, processes and tools. One common example is the AI risk impact assessment process, in which relevant questions about AI are added to existing privacy governance documentation and processes.

AI governance is still evolving, and mature AI governance programs continue to find room to innovate. As new guidance and compliance burdens emerge, alongside new and greater commercial opportunities associated with good governance, a mature AI governance program will look different in 2025 or 2026 than it did in 2024 at the same organization. Nevertheless, patterns have already emerged, especially related to the integrated nature of diverse digital teams, what governance looks like at different-sized organizations and each organization's approach for AI governance.

Research approach

Two data sources were employed in the making of this report. In the spring of 2024, the IAPP conducted its annual governance survey. The survey contained broad demographic questions, such as the size and revenue of the organization, as well as 25 questions related to AI governance. More than 670 individuals from 45 countries and territories responded. In the survey, a few questions revealed if the respondents are confident in their approach to AI governance: "Are you confident in your compliance with the EU AI Act?" and "Is your AI governance budget adequate?" Other questions were more basic: "Are you actively working on AI governance?" and "What are your challenges in reporting on or using AI?" Through these questions, we teased out subjective understanding of the maturity of an AI governance program. Some questions, like if the organization has an AI governance committee, are a sign of a mature AI governance program for a larger company but might be irrelevant for a smaller company.

A note on statistical significance: Throughout this piece, the term "significant" is only used to denote figures that are statistically significant at a 95% confidence interval ($p=0.05$).  denotes a figure that is significantly higher than the rest of the sample, and  denotes a figure that is significantly lower than the rest of the sample.



Currently, there is no clear best practice for structuring AI governance teams. Some companies embed AI governance in compliance or ethics teams, while others create stand-alone AI governance functions. AI governance is often split between multiple teams, including privacy, legal, security and risk management. As a result, AI risk impact assessments are inconsistent across organizations.

Navrina Singh
Founder & CEO, Credo AI

To complement the survey data, seven private companies with headquarters spread across North America and Europe and with business and governance practices distributed across the globe provided case studies to highlight examples of AI governance programs. The case studies describe how organizations make decisions relating to their AI governance programs, including the team's composition, their cross-functional cooperation and the tools employed. These case studies complement the insights gained from the survey data by providing individual and specific context to provide insight into the decisions made in each AI governance program. The variety of companies and their respective use of AI mirrors the diversity of approaches to governing AI, while highlighting commonalities among similar institutions.

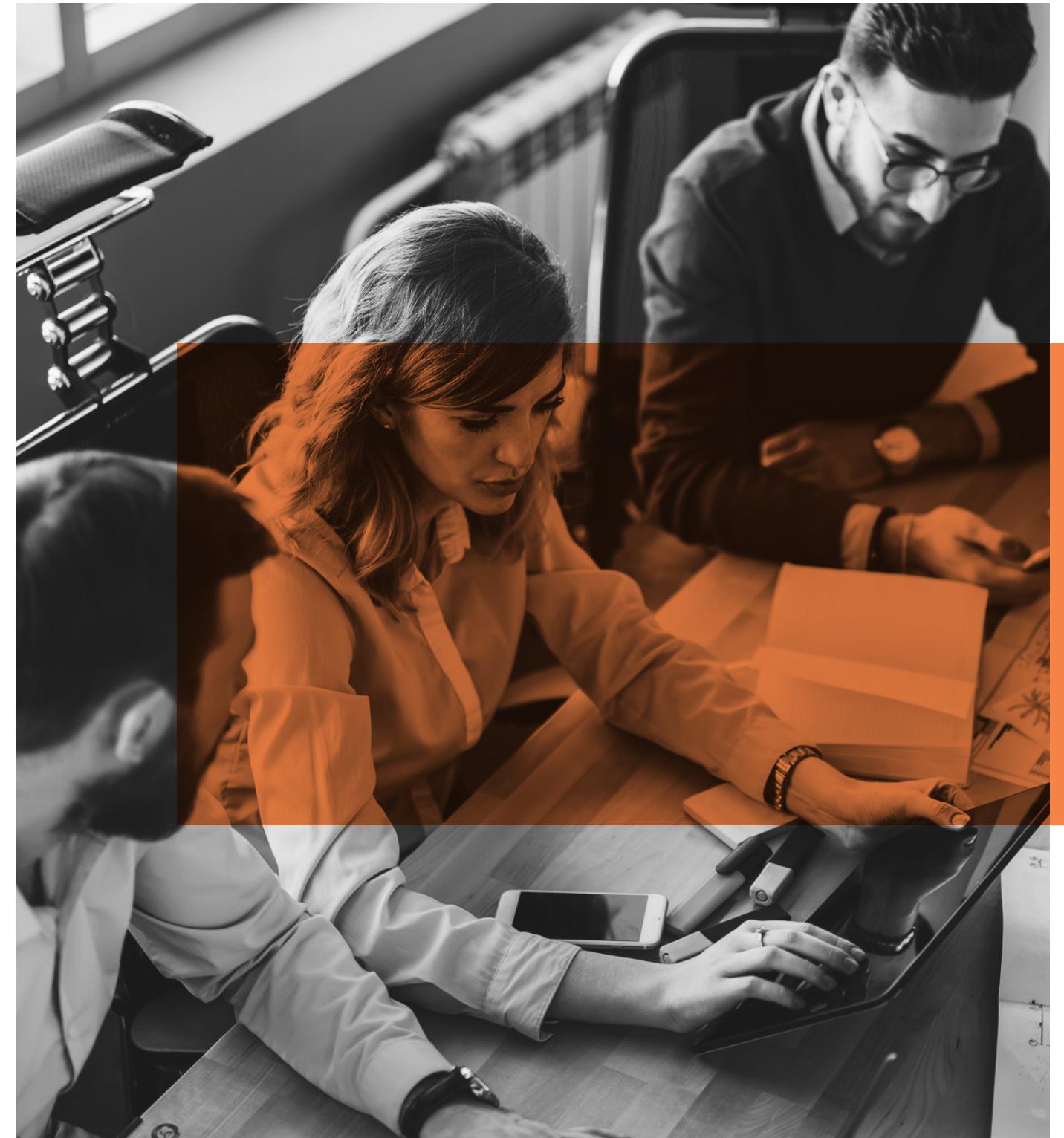
The survey data can be used to group organizations by type and size, as well as by which AI technologies an organization uses and for what purpose.



Richard Sentinella
IAPP AI Governance Center
Research Fellow



Evi Fuelle
Global Policy Director,
Credo AI

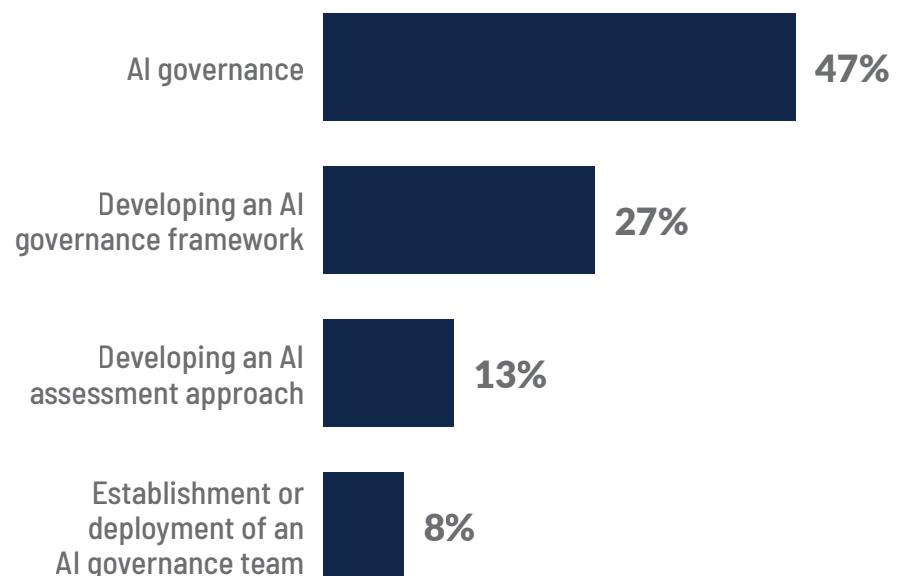


Part I. Building an AI governance program

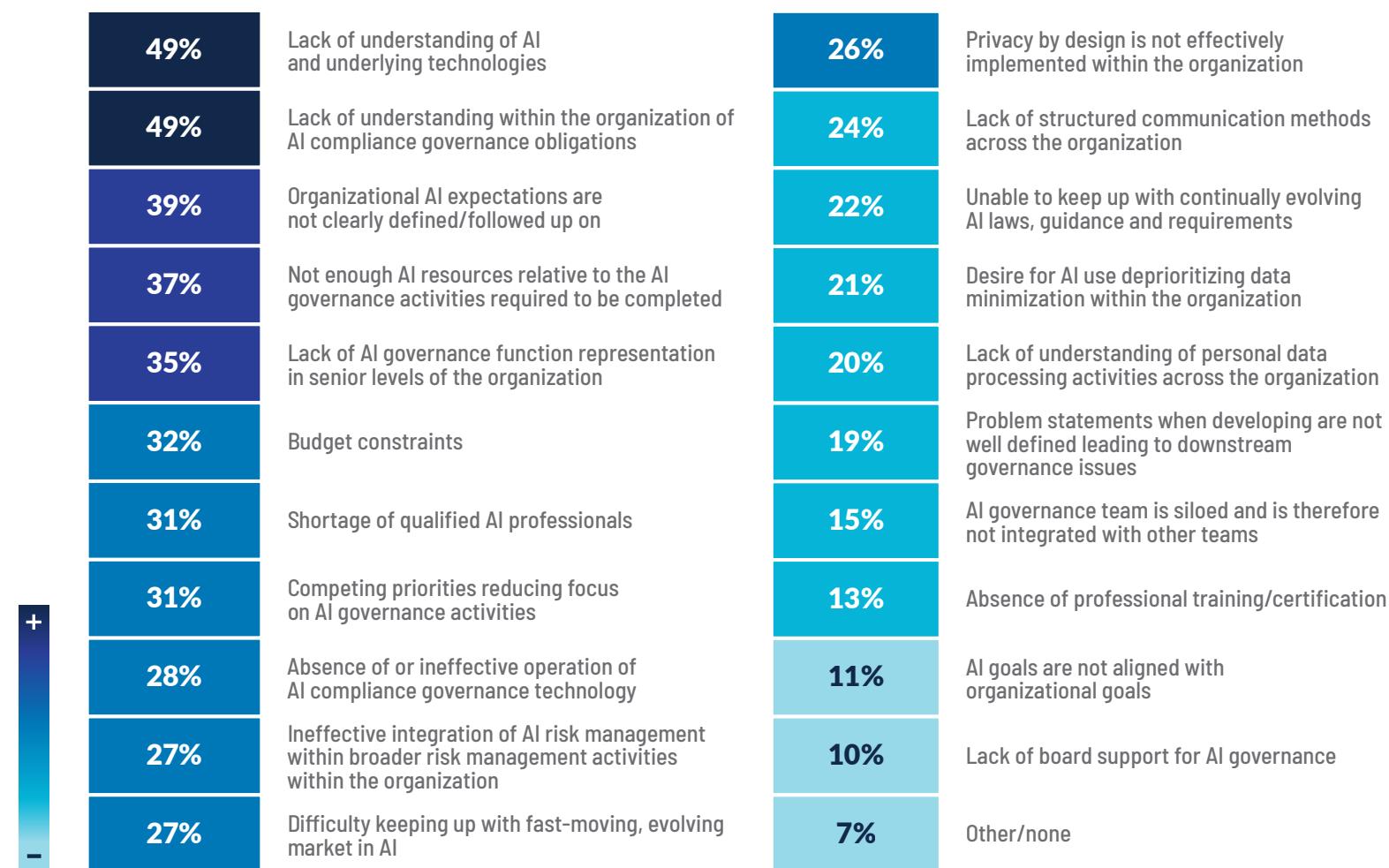
Organizations are building the foundation for compliance and strategy implementation.

Organizations using AI, which can broadly capture most analytical technologies depending on the definition, are increasingly looking to understand their compliance obligations. Many organizations use AI governance to build out a compliance program while also steering AI use toward strategic aims — from reducing headcount to increasing market competitiveness. For almost half of the respondents, AI governance was a top-five strategic priority.

Top AI-related strategic priorities for 2024



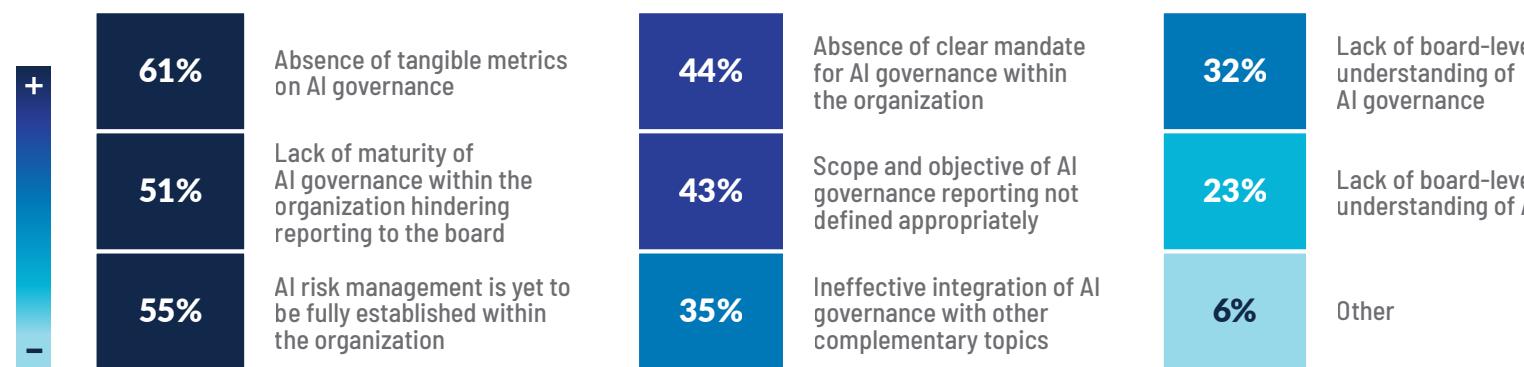
Challenges delivering on AI governance



Nevertheless, organizations face various challenges when delivering on AI governance. The largest being a lack of understanding of the underlying technologies and of AI compliance governance obligations, both at 49%. Staffing, budgets and access to resources were all significant challenges for at least a quarter of respondents.

For reporting on AI governance, the only challenge reported by less than 30% of respondents was lack of board-level understanding, which aligns with the chart above, which shows only 10% reported a lack of board support. Most organizations have upper management and board support for their AI governance initiatives — and see it as a strategic priority — but lack qualified staff, face issues with budget and resource allocation, and would benefit from increased access to training and information for AI governance.

Challenges reporting on AI governance



Top AI related strategic priorities by AI governance work

ORGANIZATION'S TOP AI RELATED STRATEGIC PRIORITIES	ORGANIZATION'S AI GOVERNANCE WORK		
	Overall	No	Yes
AI governance	47%	13% ↓	58% ↑
Developing an AI governance framework	27%	12% ↓	32% ↑
Establishing or deploying an AI governance team	8%	2% ↓	10% ↑
Developing an AI assessment approach	13%	9%	15%

AI governance is a priority

The data shows organizations using AI are more likely also to have AI governance programs, but this data does not show which came first. A pattern seems to be evolving from the case studies, which can be seen among the newer AI governance programs where AI is being used at a smaller scale and where AI governance is more documentary than professionalized and distributed. For example, companies often have a written policy but no dedicated employees until they decide to embrace AI as a strategic imperative. At that point, many organizations build out more professionalized AI governance programs, including by hiring dedicated employees, rolling out training or transferring

employees from other digital responsibility disciplines internally.

Approximately 47% of respondents reported AI governance as a top five strategic priority for their organization, while 58% of those currently working on AI governance chose it as a top priority compared to 13% of those not working on AI governance. The same holds when other responses indicate a prioritization of AI governance, for example "developing an AI governance framework" and "establishing or deploying an AI governance team." Privacy functions also reported similar AI governance prioritization, with 59% gaining additional responsibility for AI governance.

Approximately 47% of respondents reported AI governance as a top five strategic priority for their organization, while 58% of those currently working on AI governance chose it as a top priority compared to 13% of those not working on AI governance.



Revenue of organization in USD by AI use

ORGANIZATION'S ANNUAL REVENUE	ORGANIZATION CURRENTLY USES AI FOR									
	Overall	Process automation	Automated decision-making	Data analysis	Personalizing experiences	Customer interactions	Other	Not currently but expected to use AI within the next 12 months	Not currently using AI	Unsure
Less than \$100 million	20%	12%	12%	13%	14%	11%	22%	24%	40%	21%
\$101-\$999 million	26%	23%	17%	26%	21%	23%	31%	32%	35%	7%
\$1-\$8.9 billion	29%	32%	29%	30%	32%	34%	29%	24%	14%	52%
\$9-\$19.9 billion	10%	13%	16%	13%	12%	9%	6%	13%	2%	7%
\$20-\$59.9 billion	8%	10%	13%	10%	13%	11%	6%	6%	5%	10%
More than \$60 million	6%	10%	13%	8%	9%	12%	6%	2%	4%	3%

Larger companies are more likely to use AI and AI governance programs.

AI use is more common among larger organizations. This is not necessarily surprising, as the largest companies arguably have the most to gain by using AI and the most to lose by forgoing or mismanaging its use. When looking at markers of AI governance maturity, such as confidence in compliance with the EU AI Act, maturity is also correlated with a larger corporate environment. In other words, organizations with greater revenue, sufficient budgets and heightened regulatory risk exposures are more highly correlated with mature AI governance programs.

When looking at how organizations use AI and how many countries they operate in, number of employees, or annual revenue, there are clear trends. The smallest organizations are underrepresented among respondents using AI to drive process automation, automated decision-making, data analysis, personalized experiences or customer interactions. They are overrepresented among those not currently using AI. The opposite is mostly true for larger companies. However, some smaller companies that develop AI solutions as their primary business activity buck this trend.



Headcount of organization by AI use

ORGANIZATION'S TOTAL NUMBER OF EMPLOYEES	ORGANIZATION CURRENTLY USES AI FOR									
	Overall	Process automation	Automated decision- making	Data analysis	Personalizing experiences	Customer interactions	Other	Not currently but expected to use AI within the next 12 months	Not currently using AI	Unsure
Fewer than 100	8%	4%	3%	4%	6%	3%	10%	9%	28%	0%
100-999	20%	13%	12%	15%	12%	11%	25%	30%	32%	17%
1,000-4,999	26%	26%	18%	26%	24%	28%	28%	31%	19%	28%
5,000-24,999	23%	27%	30%	28%	27%	26%	22%	15%	14%	28%
25,000-79,999	11%	13%	17%	12%	17%	14%	7%	11%	0%	21%
More than 80,000	11%	17%	20%	15%	14%	17%	7%	5%	7%	7%

Number of countries of operation by AI use

ORGANIZATION'S NUMBER OF COUNTRIES OF OPERATION	ORGANIZATION CURRENTLY USES AI FOR									
	Overall	Process automation	Automated decision- making	Data analysis	Personalizing experiences	Customer interactions	Other	Not currently but expected to use AI within the next 12 months	Not currently using AI	Unsure
1	27%	20% ↓	20% ↓	18% ↓	14% ↓	15% ↓	29%	43% ↑	51% ↑	28%
2-5	19%	16%	14%	17%	16%	18%	18%	19%	14%	10%
6-10	13%	12%	8%	14%	17%	13%	12%	13%	12%	10%
11-20	10%	12%	12%	12% ↑	10%	12%	13%	7%	7%	7%
21-40	11%	11%	12%	12%	13%	14%	15%	8%	9%	17%
41-60	6%	7%	7%	7%	10% ↑	7%	4%	5%	2%	10%
More than 60	15%	23% ↑	27% ↑	20% ↑	21% ↑	20% ↑	9%	6% ↓	5% ↓	17%

Revenue of organization in USD by AI governance work

ORGANIZATION'S ANNUAL REVENUE	ORGANIZATION'S AI GOVERNANCE WORK		
	Overall	No	Yes
Less than \$100 million	20%	39%	15%
\$101-\$999 million	26%	31%	25%
\$1-\$8.9 billion	29%	20%	32%
\$9-\$19.9 billion	10%	6%	11%
\$20-\$59.9 billion	8%	4%	9%
More than \$60 billion	6%	1%	8%

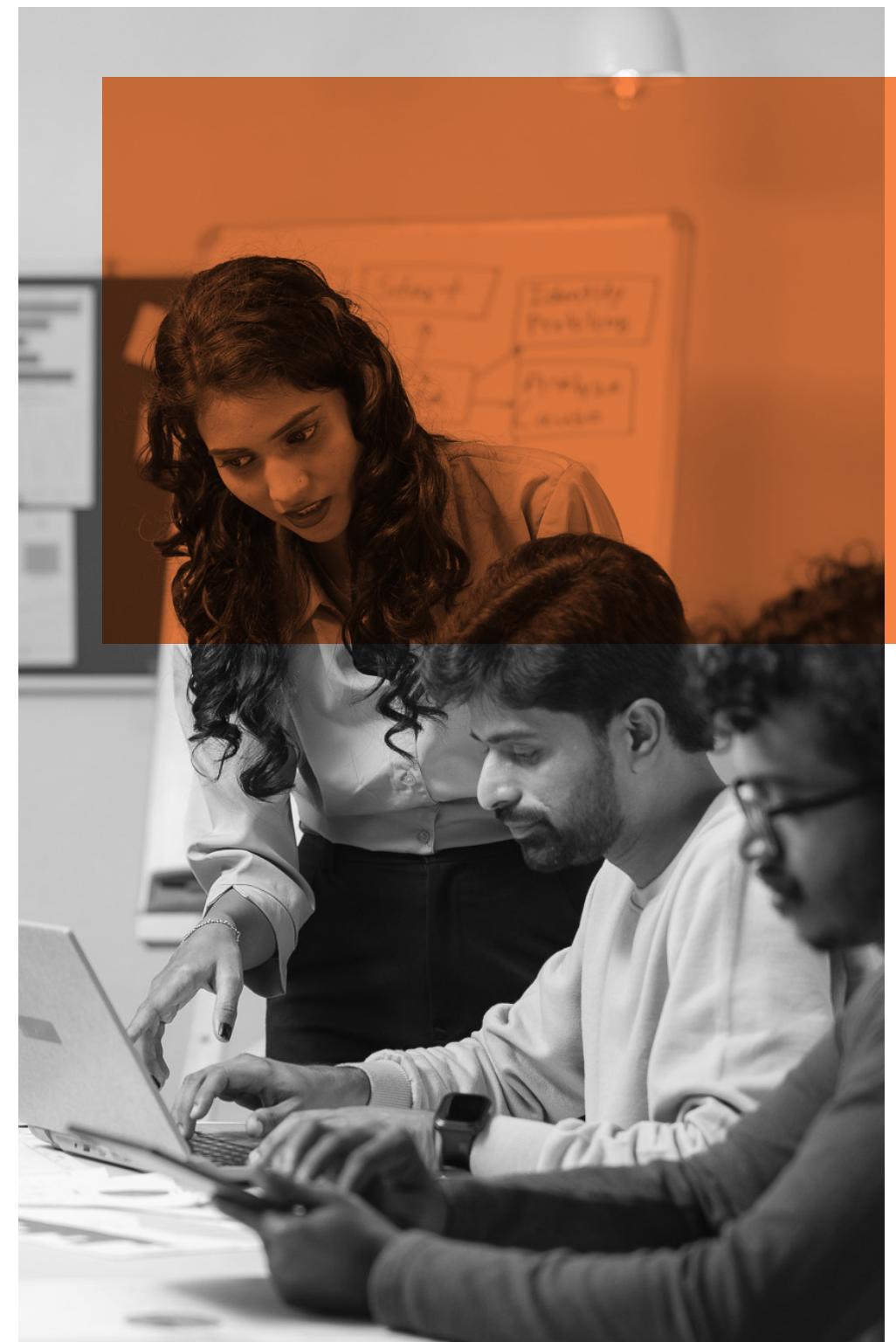
While 20% of respondents work at organizations with annual revenues of less than USD100 million, respondents at these organizations made up 39% of the population who said they are not actively working on AI governance and only 15% of those who are.

Headcount by AI governance work

ORGANIZATION'S GLOBAL HEADCOUNT	ORGANIZATION'S AI GOVERNANCE WORK		
	Overall	No	Yes
Fewer than 100	8%	20%	5%
100-999	20%	32%	17%
1,000-4,999	26%	20%	28%
5,000-24,999	23%	21%	24%
25,000-79,999	11%	3%	13%
More than 80,000	11%	3%	13%

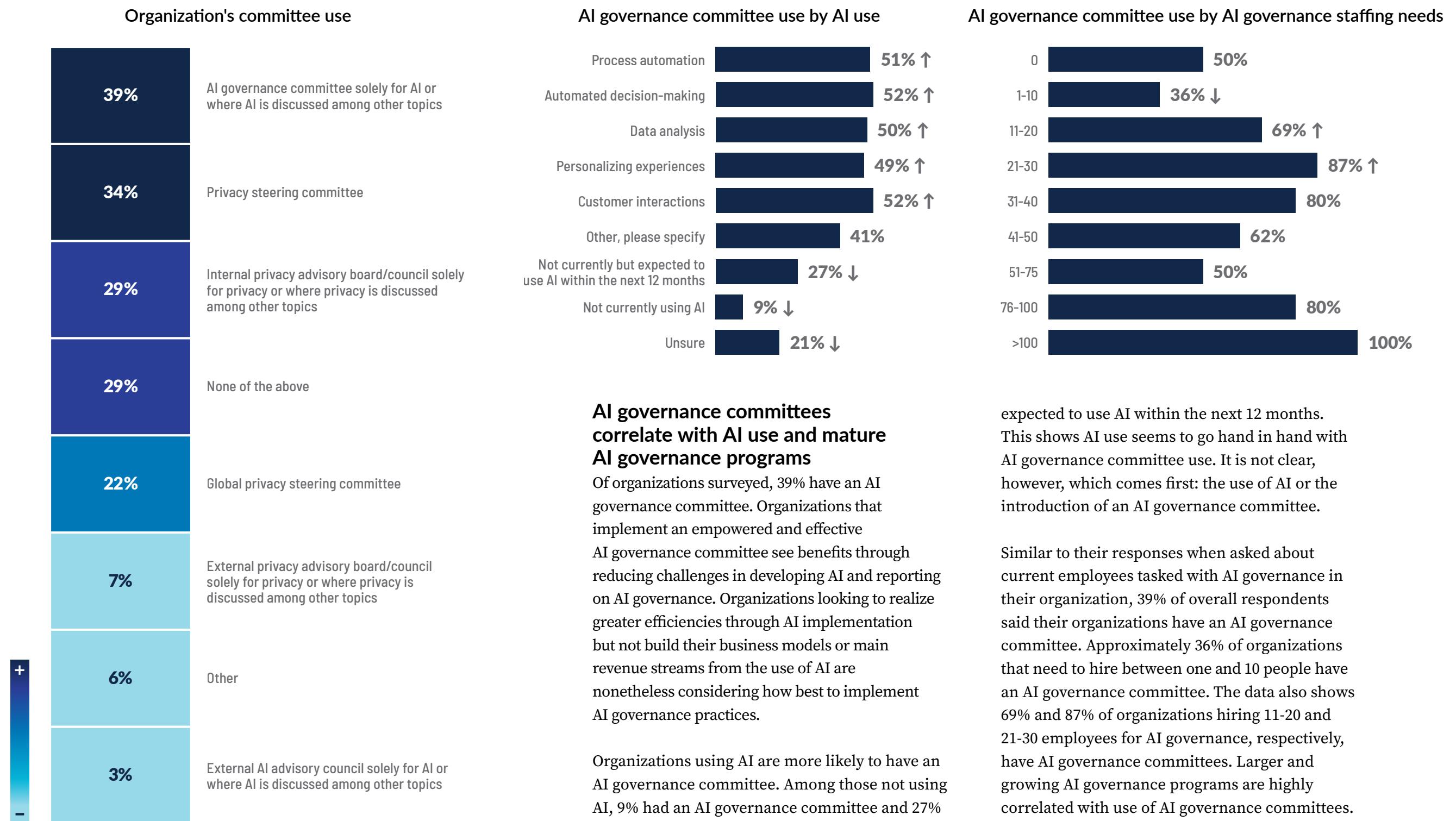
Larger organizations more likely to involve more functions in AI

Teams with one to 10 AI governance professionals are less likely to increase collaboration among functions in a statistically significant manner, but teams with more than 11 AI governance professionals are more likely to collaborate. This same trend is even more apparent when looking at the expected growth of AI governance professionals. Teams adding between one and 10 employees are less likely to collaborate, and those adding more than 11 are more likely to collaborate.



Functions with additional AI governance responsibility by AI governance staffing and needs

FUNCTIONS THAT WILL HAVE ADDITIONAL INVOLVEMENT IN AI GOVERNANCE	PEOPLE TASKED WITH AI GOVERNANCE								PEOPLE NEEDED FOR AI GOVERNANCE IN THE NEXT YEAR									
	Overall	1-10	11-20	21-30	31-40	41-50	51-75	100	0	1-10	11-20	21-30	31-40	41-50	51-75	76-100	>100	
Privacy	57%	58%	76% ↑	60%	100%	40%	50%	33%	60%	53% ↓	73% ↑	67%	100% ↑	54%	50%	60%	50%	
Legal and compliance	55%	56% ↓	64%	70%	67%	80%	88%	100%	40%	53%	60%	73%	80%	54%	100%	100% ↑	50%	
Security	53%	54% ↓	69%	60%	33%	80%	75%	67%	10% ↓	50% ↓	70% ↑	73%	40%	62%	100%	80%	50%	
Product development	25%	25% ↓	42% ↑	40%	0%	60%	50%	67%	20%	22% ↓	34%	73% ↑	0%	31%	50%	60%	50%	
Marketing	13%	14%	16%	20%	33%	40%	25%	33%	10%	11% ↓	20%	20%	20%	15%	50%	40%	50%	
Human resources	21%	20% ↓	33%	50% ↑	33%	60% ↑	38%	33%	20%	16% ↓	33% ↑	53% ↑	60% ↑	31%	50%	40%	50%	
Customer support	10%	9% ↓	16%	40% ↑	33%	40% ↑	25%	33%	10%	8% ↓	16%	33% ↑	20%	23%	50%	40% ↑	50%	
Information technology	52%	52%	58%	60%	33%	100%↑	75%	100%	50%	51%	53%	60%	80%	54%	100%	60%	100%	
Data governance	44%	44% ↓	62% ↑	70%	33%	60%	50%	100%	50%	41% ↓	58% ↑	53%	60%	54%	50%	60%	50%	
Risk management	40%	39% ↓	58% ↑	60%	33%	40%	38%	67%	20%	37% ↓	51% ↑	47%	60%	54%	100%	60%	0%	
Vendor management	24%	23% ↓	42% ↑	60% ↑	33%	60%	38%	33%	10%	21% ↓	31%	60% ↑	40%	38%	100% ↑	40%	50%	
Executive leadership	38%	40%	49%	50%	0%	60%	38%	33%	40%	37%	43%	60%	20%	54%	50%	40%	0%	
Public relations/communications	7%	7%	9%	30% ↑	0%	40% ↑	25%	0%	0%	4% ↓	15% ↑	33% ↑	20%	8%	50% ↑	20%	50% ↑	
Audit/internal control	25%	25%	27%	50%	33%	40%	38%	100%↑	20%	22% ↓	28%	33%	60%	46%	50%	60%	50%	
Ethics and compliance	35%	35% ↓	58% ↑	60%	67%	40%	38%	67%	40%	30% ↓	53% ↑	60% ↑	80% ↑	38%	100%	80% ↑	0%	
Other, please specify	4%	4%	7%	20% ↑	0%	0%	0%	0%	10%	3%	6%	7%	0%	8%	0%	20%	0%	
None	2%	1%	0%	0%	0%	0%	0%	0%	10% ↑	2%	1%	0%	0%	0%	0%	0%	0%	



While 39% of respondents said their companies have an AI governance committee, only 5% not working on AI governance said their companies have a committee and 49% working on AI governance said their companies have a committee in place.

Having an AI governance committee is less correlated with issues developing AI, including organizational AI expectations at 43% and AI governance representation at 39%.

Respondents at organizations with AI governance committees were less likely to report challenges in AI governance reporting, including lack of a clear mandate at 41% and of board-level understanding in both AI use at 40% and AI governance at 37%.

AI governance committee use by AI governance use

Not currently working on AI governance 5% ↓

Currently working on AI governance 49% ↑

AI governance committee use by challenges delivering AI governance

Lack of understanding of AI and underlying technologies 45%

Lack of AI governance function representation in senior levels of the organization 39% ↓

Organizational AI expectations are not clearly defined/followed up on 43% ↓

Lack of understanding within the organization of AI compliance governance obligations 47%

Shortage of qualified AI professionals 49%

Budget constraints 46%

Not enough AI resources relative to the AI governance activities required to be completed 51%

Competing priorities reducing focus on AI governance activities 48%

AI governance committee use by challenges reporting on AI governance

Lack of board-level understanding of AI 40% ↓

Lack of board-level understanding of AI governance 37% ↓

Absence of tangible metrics on AI governance 50%

Absence of clear mandate for AI governance within the organization 41% ↓

Ineffective integration of AI governance with other complementary topics 50%

Scope and objective of AI governance reporting not defined appropriately 50%

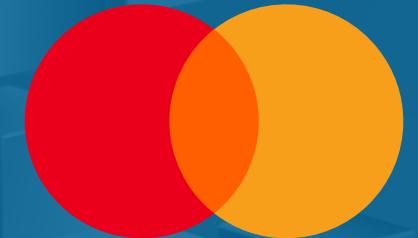
Lack of maturity of AI governance within the organization hindering reporting to the board 50%

AI risk management is yet to be fully established within the organization 49%

Other 57%

Case study: AI governance at Mastercard

Mastercard is a global technology company in the payments industry, whose logo is ubiquitous and likely on a card in many of our wallets. With a business model grounded in the processing of transaction data, the company has long been active in data privacy and cybersecurity. Banking and financial services have historically been highly regulated, meaning the company is used to staying on top of regulations and compliance efforts. Given Mastercard's reach and size, its governance systems must be both formalized and well-coordinated to meet the highest standards.



Its AI governance efforts were born out of the privacy and data strategy functions. Both functions worked together during initial EU General Data Protection Regulation compliance efforts, and they identified the strategic importance of AI and the need to build an AI governance framework early on. In 2022, after almost five years of intense cooperation, the teams were brought together into a centralized and coordinated AI governance program.

This core AI governance team has specialists with many different skills, including lawyers, compliance officers, policy experts and data scientists, and works closely with other teams, such as technology and corporate security. It works with every department through their AI risk assessment and mitigation process, which screens the different AI initiatives within the company. This process is integrated into the company's larger risk management framework. The team focuses its efforts on higher risk cases that use personal information or that may impact people, society or the company's reputation.

The screening and prioritizing of initiatives is guided by Mastercard's policies. During the AI risk assessment and mitigation process, experts from other teams are brought in as needed, depending on the risks identified. Anything deemed potentially high risk is reviewed by the AI and Data Council, which is made up of senior leaders from a variety of functions and co-chaired by the chief privacy officer and chief AI and data officer. The core team, along with the council, advises the different functions with concrete actions needed to mitigate risks. For example, if there is a potential intellectual property risk, an IP lawyer will be brought in to consult. The team might require guidance from other disciplines outside of the core team's scope, such as cybersecurity, technology or antitrust. It has started adding skills that were previously not available within the current AI governance team or other functions, hiring staff with new skills or upskilling their current employees.

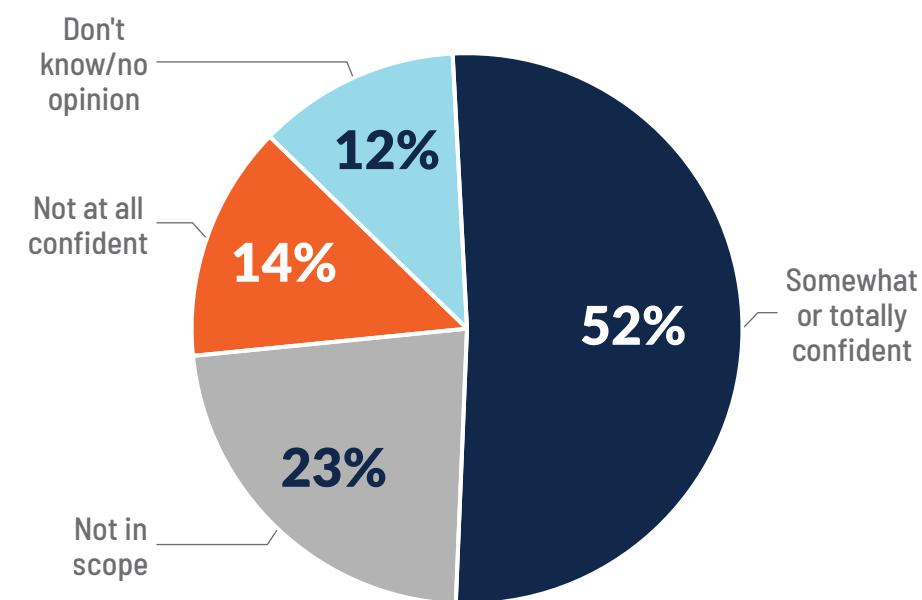
The company provides training to employees outside the core function focused on growing awareness of how to operationalize its Data & Tech Responsibility Principles through its AI governance policies and processes. The company benefits from the culture of compliance it has cultivated, which is grounded in a commitment that employees at all levels will do what it takes to ensure compliance with regulations and internal AI use policies, including the principles mentioned above.

Mastercard's culture, ubiquity and role in financial services has shaped how it approaches governing AI. Its global reach and structure means it quickly needed to build on other formalized processes and make sure everything is well documented. Its small team can cover a lot of ground due to its streamlined processes and ability to tap on experts throughout or beyond the organization as needed.

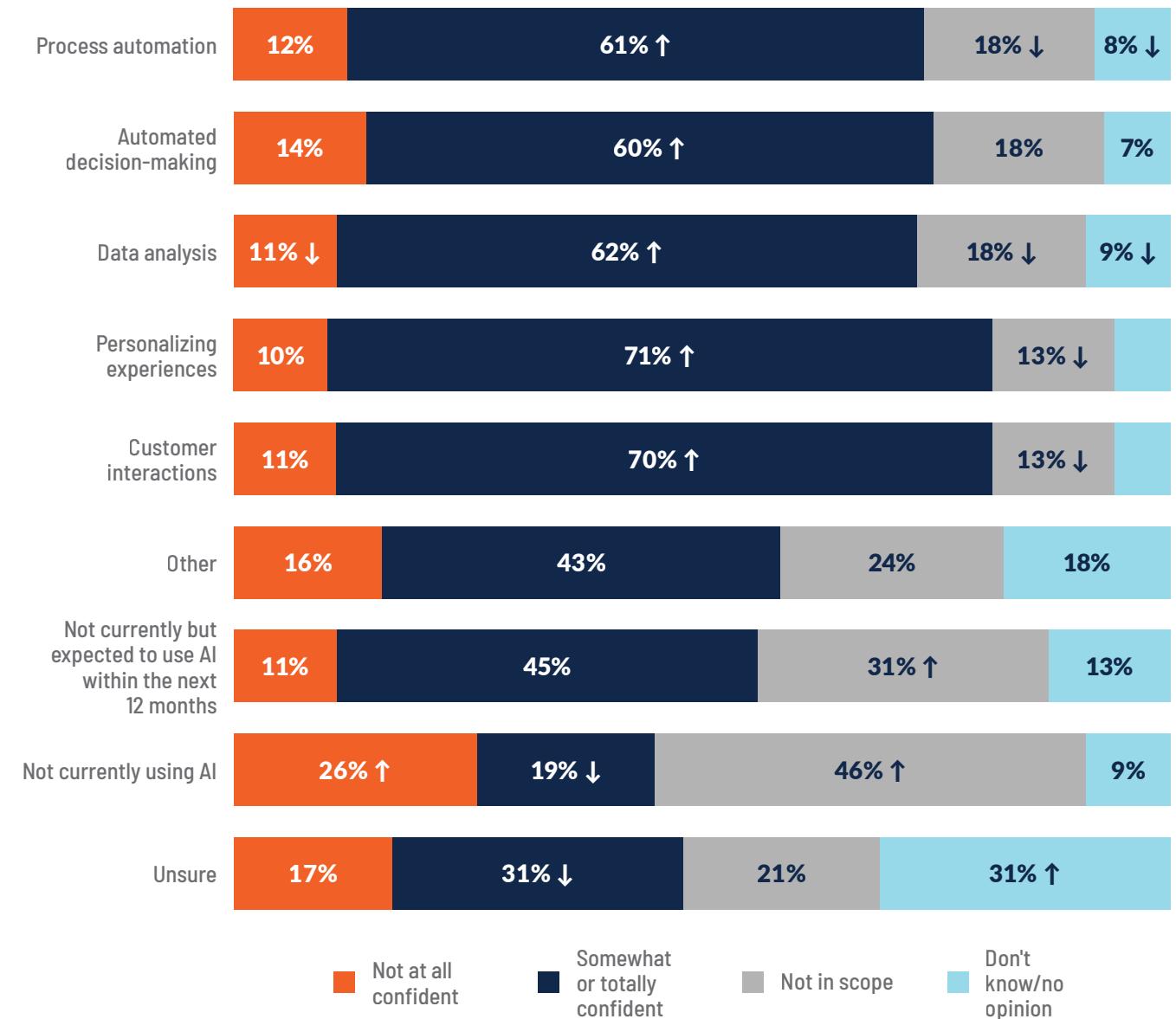
Higher confidence in ability to comply with the AI Act

While 52% of the respondents were somewhat or totally confident in their organization's ability to comply with the AI Act, this number rose moderately among those using AI for process automation at 62%, automated decision-making at 60% and data analysis at 62%. Confidence increased for those using AI for personalizing experiences at 71% and customer interaction at 70%. The organizations in the latter cases could be caught up on compliance requirements, leading to increased confidence.

Confidence in organization's ability to be compliant with the EU AI Act



EU AI Act compliance confidence by AI use



Case study: AI governance at TELUS

TELUS is a Canadian communications technology provider. The company recently expanded and diversified its business by providing connectivity and technology to drive meaningful change, from transforming health care to making the world's food supply more sustainable.



The innovative culture at TELUS has helped it embrace the use of generative AI. The company, and particularly its Data & Trust Office, embraced the explosion of interest in generative AI to innovate safely, rejecting the idea there is a need to balance innovation with safety; to innovate well, you need safety. With the impact of data and AI technology felt broadly, the company ensures its work reflects society's diversity by engaging every team member in data and AI literacy offerings, as well as offering additional opportunities to upskill, benefiting the individual, the business and society more broadly.

The company has a history of developing new technologies that required it to consider data ethics, data governance and privacy, which meant these teams already collaborated well and could quickly address any new challenges when AI governance became a consideration. As a result, this institutional maturity made it easier to embrace new AI systems while ensuring control over the organization's data. When generative AI applications became available for public use, the DTO quickly developed policies and trainings, based on existing principles and processes such as its [Trust Model](#). These were designed to

protect TELUS customers, team members and the brand. The DTO also developed a comprehensive communications strategy to educate and build confidence among its team members.

Over time, the DTO worked with its technology team counterparts to build out the company's software platform, which allowed employees to access a variety of approved tools. AI models made by external providers were available on this platform, but they were managed and controlled by TELUS. Any data put into the models would be reliably safeguarded by virtue of their own platform hosting the models, as well as the agreements made with the providers of the models. Its first public-facing generative AI tool, a customer support tool, was the first generative AI in the world to be certified as privacy by design by the International Organization for Standardization. The DTO is working on additional AI certifications.

TELUS' company-wide data culture instills innovation and safety throughout every facet of the organization. Beyond the data and AI literacy programming available to all team members

regardless of their roles, three different programs are offered with varying levels of formality to further upskill and ensure data governance processes are highly agile: data stewardship, purple team testing and the Responsible AI Squad. The wide variety of ways the team can engage with data and AI, as well as interact with and give feedback to the DTO, shows its commitment to put customers and communities first is not siloed in the privacy office but is part of its corporate culture.

Data stewards are in-business data leaders appointed by executives throughout each area of the company who are given special training so they can act as data initiative champions and data experts for their teams. For example, data stewards can work with their teams to submit AI impact assessments and help them determine what datasets are available and how to leverage them responsibly. When the DTO needs to disseminate information to the different departments, the data stewards are often asked to support the effort, allowing for agility within their data programs. The Purple Team is in reference to "purple teaming," a collaborative approach to identify both weaknesses and

mitigations through adversarial testing to support the robustness of an application. It combines blue teaming, which conducts vulnerability evaluations and provides mitigation techniques, and red teaming, which adopts an attacker's mindset and methods to adversarially test an application and find vulnerabilities. Any team member can join the Purple Team to gain access to new tools, skills and participate in testing AI systems for both functionality and fragility. This diverse group and open exercise helps the DTO and the broader business gain large amounts of data on safety and functionality before releasing tools for all employees or customers, while also creating additional buy-in among stakeholders that the tools will not be released until proven safe.

AI governance is supported through a Responsible AI Squad, which grew from an informal gathering of AI engineers, policy professionals and risk professionals who wanted to support the commitment to responsible AI. The squad regularly interacts during monthly meetings to review and assess new uses of AI or situations that can benefit from a collaborative group.

When asked about the sufficiency of the current AI governance budget relative to their organization's obligations and objectives, 18% were satisfied and 64% were not satisfied.

Organizations with larger budgets have greater AI governance maturity

Larger organizations tend to have higher budgets for AI governance. Organizations with more employees are more likely to have larger budgets as well.

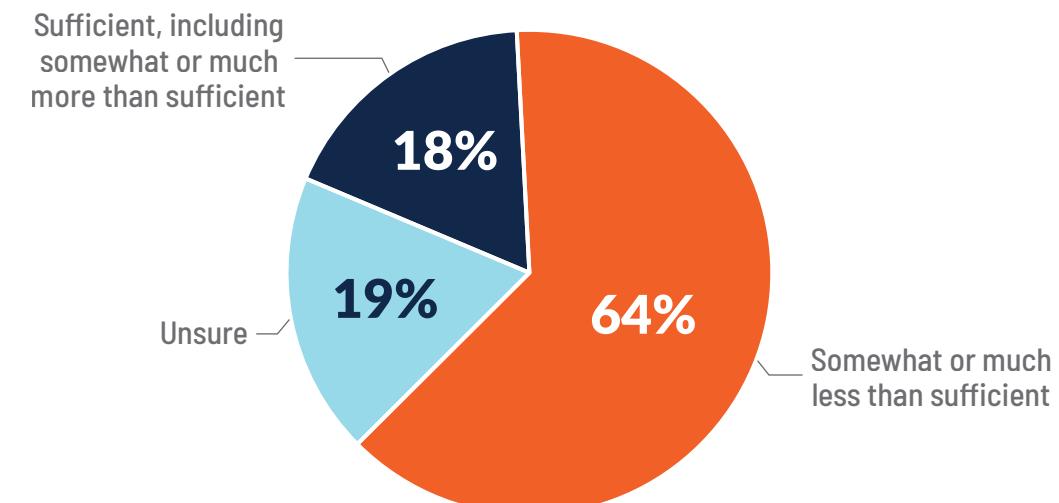
When asked about the sufficiency of the current AI governance budget relative to their organization's obligations and objectives, 18% were satisfied and 64% were not satisfied. This question has a very strong correlation with the challenges organizations are facing. Those who feel their company has challenges in delivering AI also feel its AI governance efforts are underfunded.

Those working at companies with budgets less than USD100,000 were significantly more likely to be unsure about the sufficiency of their budgets and were less likely to say it is sufficient. The data does not show a significant easing of budget concerns until it reaches USD1 million-USD4.9 million, at which point 55% of respondents are likely to say the budget is insufficient while 27% say it is sufficient. Budgets higher than USD5 million show the same pattern.

Headcount by AI governance budget in USD

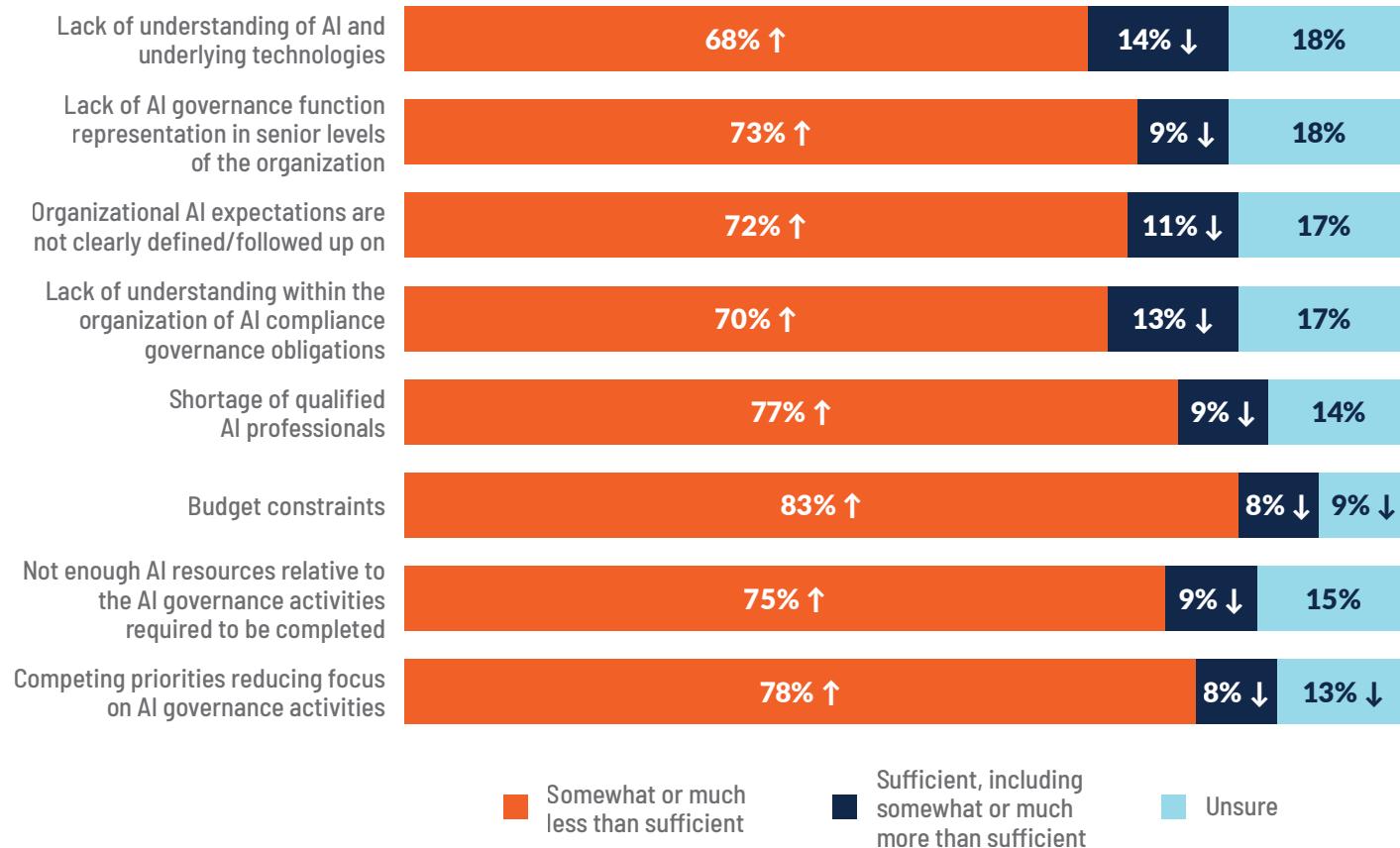
ORGANIZATION'S HEADCOUNT	ORGANIZATION'S AI GOVERNANCE BUDGET				
	Overall	Less than \$100,000	\$100,000-\$999,999	\$1 million-\$4.9 million	More than \$5 million
Fewer than 100	8%	4%	0%	0%	4%
100-999	20%	7%	0%	0%	7%
1,000-4,999	26%	35%	23%	0%	35%
5,000-24,999	23%	27%	21%	8%	27%
25,000-79,999	11%	16%	26%	8%	16%
More than 80,000	11%	11%	31%	85%	11%

How would you describe your company's AI governance budget with respect to its AI governance obligations and objectives?

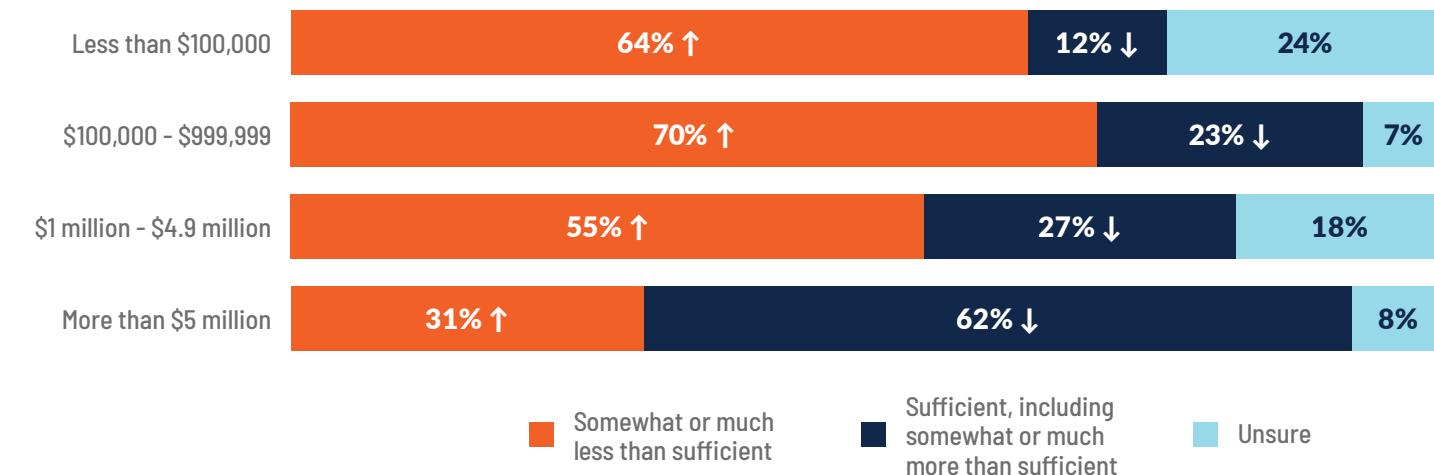


Those working at companies with budgets less than USD100,000 were significantly more likely to be unsure about the sufficiency of their budgets and were less likely to say they are sufficient. The data does not show a significant easing of budget concerns until it reaches USD1 million-USD4.9 million, at which point 55% of respondents are likely to say the budget is insufficient while 27% say it is sufficient. Budgets higher than USD5 million show the same pattern.

AI governance budget sufficiency by challenges delivering AI



AI governance budget sufficiency by AI governance budget in USD





Case study: AI governance at Boston Consulting Group

Boston Consulting Group provides management consulting services and technology solutions to clients around the world. To manage the risks associated with the AI systems it delivers to clients and deploys internally, it has developed a comprehensive risk management process.

To manage this process, BCG knew it wanted an integrated tool that would help facilitate its AI risk management from ideation to delivery. Extensive benchmarking of commercially available solutions revealed no out-of-the box tools met its needs. As a result, the company decided to build a tool to help it manage various digital risks, resulting in the risk management tool.

The tool catalogs all internal and client projects. Even before a project starts, the AI risk management process begins by developing an initial risk landscape of the use case, giving consultants an initial assessment of risks and mitigations and guardrail requirements for each prospective project. Once the project moves forward, a full impact assessment is conducted. BCG evaluates business, technical, infosecurity, data protection, legal and responsible AI risks. The risks identified inform the team about the mitigation and guardrail measures that must be implemented during the development phase.

The team takes special care when developing high-risk use cases. These encompass legally defined high-risk AI systems

or consequential decision-making systems, but they go further to also include specially defined cases, such as AI use cases that may involve children. BCG's Responsible AI Policy informs the risk management process, including which use cases are categorized as high risk. Both the risk management process and the Responsible AI Policy are overseen by the chief AI ethics officer and the Responsible AI Council, which is made up of fixed and rotating senior-level executives from across the organization, providing review and guidance for all high-risk use cases.

During this process, the tool is used by the Responsible AI Team, as well as specialists on other functional teams. At different points in the risk management process, specialists from engineering, infosecurity, data protection, legal, and risk and compliance functions evaluate risks and provide guardrails and mitigations, which are captured in the risk management tool. By having multiple teams interact and collaborate through the use of the risk management tool, BCG has been able to find a common language around how risks are defined and actioned, as well as establish a single source of truth for the full risk landscape on a project.

Inside the tool exists the ground truth for the company's projects, where all relevant data around risk and mitigation efforts live. As new risks are identified during the development phase and mitigation measures are implemented, these updates are recorded in the tool by the relevant functional team. Project executive sponsors can see which cases are being developed and the associated risks and mitigation efforts in real time, allowing them to track changes in risk profiles as they evolve. It is also possible for system cards or other project documents to be formatted and exported from the tool.

BCG is unique in the use of its risk management tool in many ways. As it is using the risk management tool and process for all types of digital risk management and for AI systems developed for internal and client use, the process is used often enough that it warranted investment in building a customized tool. Because it maintains the system itself, it can more easily adapt the tool, for example if additional questions need to be added to the impact assessment questionnaire. This customization allows the company to integrate the tool into multiple processes and build capabilities to share data when necessary, making reporting an automated feature once set up.

Part II. Professionalizing AI governance

Organizations see hiring AI governance professionals as an important part of professionalizing an AI governance program.

When starting an AI governance program, one of the first steps an organization must undertake is finding the right skills to run the program effectively. In 2024, AI governance saw a mix of both giving responsibilities to those already involved in a digital responsibility discipline, like privacy or data governance, while hiring for new skills like red teaming.

Most AI governance teams are small and, at the time the survey data was collected, there was no indication that these teams will grow significantly in 2025. The largest headcount increases are seen at organizations with large teams, budgets and general sizes. These larger organizations are also likely to have greater specialization within their teams and more formalized approaches to AI governance. Smaller organizations will likely hire more senior generalists to start their AI governance programs.

AI governance professional recruitment by AI governance use

WHICH TYPES OF RESOURCES AND ASSOCIATED SKILL SETS IS YOUR ORGANIZATION CURRENTLY RECRUITING FOR?	AI GOVERNANCE USE	
	Overall	Not currently working on AI governance
AI governance professional	8%	3% ↓

ORGANIZATION'S STRATEGIC PRIVACY PRIORITIES RELATING TO AI GOVERNANCE	PEOPLE NEEDED FOR AI GOVERNANCE IN THE NEXT YEAR									
	Overall	0	1-10	11-20	21-30	31-40	41-50	51-75	76-100	>100
AI governance	47%	20% ↓	50% ↓	63%	67%	60%	54%	50%	100% ↑	100%
Developing an AI governance framework	27%	0% ↓	31%	26%	13%	80% ↑	54%	100% ↑	20%	0%
Establishing or deploying an AI governance team	8%	0%	7% ↓	20% ↑	13%	0%	23%	0%	0%	0%
Developing an AI assessment approach	13%	0%	14%	19%	13%	20%	8%	0%	40%	0%

Organizations in North America have larger AI governance teams than Europe

Organizations working on AI are hiring AI governance professionals at a significantly faster rate at 10% than those not working on AI at 3%. This could mean AI governance professionals are being drawn from other digital responsibility disciplines internally.

Organizations not hiring AI governance professionals in the next twelve months are statistically underrepresented among those who care about AI governance, as indicated by 20% of respondents. Among organizations that see AI governance or developing an AI governance framework as a top-five strategic priority, there is a general trend toward hiring larger amounts of staff.

According to the data, organizations may be predisposed to hire AI governance employees and to hire a certain amount based on if their headquarters are in North America, the seniority of the most senior AI governance employee and AI governance maturity. European organizations, on the other hand, are less likely than their North American counterparts to hire AI governance employees.

North American organizations are overrepresented among organizations hiring 11-20 or 21-30 employees for AI governance, at 79% and 93% respectively, compared to 65% of organizations overall. On the other hand, organizations with their primary location in Europe make up 24% of respondents. They are slightly overrepresented in organizations hiring one to 10 staff at 25% and underrepresented among organizations hiring 11-20 staff at 13%.

“

The (AI Governance Professional) is a certification that stands out when recruiting new staff. This is true despite your background, which might be in law, compliance or project management. In all cases, having the AIGP would help position you well amongst other candidates that are searching for roles in AI governance.

Heather Domin, AIGP
Vice President and Head of Office of Responsible AI and Governance, HCLTech

Geographical distribution by AI governance staffing and AI governance staffing needs

PRIMARY LOCATION OF ORGANIZATION'S HEADQUARTERS	PEOPLE TASKED WITH AI GOVERNANCE								PEOPLE NEEDED FOR AI GOVERNANCE IN THE NEXT YEAR								
	Overall	1-10	11-20	21-30	31-40	41-50	51-75	100	0	1-10	11-20	21-30	31-40	41-50	51-75	76-100	>100
North America	65%	65% ↓	91% ↑	80%	33%	40%	50%	100%	60%	62% ↓	79% ↑	93% ↑	40%	62%	50%	100%	50%
Europe	24%	24% ↑	4% ↓	10%	67%	60% ↑	50%	0%	30%	25% ↑	13% ↓	7%	60%	23%	50%	0%	50%
South America	1%	0%	2%	0%	0%	0%	0%	0%	0%	1%	1%	0%	0%	0%	0%	0%	0%
Africa	1%	1%	0%	0%	0%	0%	0%	0%	10% ↑	1%	3%	0%	0%	0%	0%	0%	0%
Asia	5%	4%	2%	10%	0%	0%	0%	0%	0%	6%	3%	0%	0%	15%	0%	0%	0%
Oceania	4%	5%	0%	0%	0%	0%	0%	0%	0%	5%	3%	0%	0%	0%	0%	0%	0%

North American organizations are overrepresented among organizations hiring 11-20 or 21-30 employees for AI governance, at 79% and 93% respectively, compared to 65% of organizations overall. On the other hand, organizations with their primary location in Europe make up 24% of respondents, they are slightly overrepresented in organizations hiring one to 10 staff at 25% and underrepresented among organizations hiring 11-20 staff at 13%.

Revenue of organization by most senior AI governance employee reporting

ORGANIZATION'S ANNUAL REVENUE IN USD	MOST SENIOR AI GOVERNANCE EMPLOYEE ULTIMATELY REPORTS TO:													
	Overall	General counsel/head of legal	CEO	Chief compliance officer	Chief operating officer	Chief information officer	Chief technology officer	Chief information security officer	Chief risk officer	Chief financial officer	Chief people officer/head of HR	Chief consumer officer/head of customer	Chief product officer	Other
Less than \$100 million	20%	8%	37%	5%	14%	4%	10%	10%	5%	29%	0%	0%	30%	18%
\$101-\$999 million	26%	36%	31%	5%	9%	20%	23%	23%	32%	35%	100%	0%	20%	18%
\$1-\$8.9 billion	29%	33%	17%	51%	41%	41%	26%	42%	27%	29%	0%	0%	30%	26%
\$9-\$19.9 billion	10%	11%	5%	16%	14%	11%	16%	13%	14%	0%	0%	0%	10%	18%
\$20-\$59.9 billion	8%	5%	8%	11%	5%	13%	19%	10%	5%	6%	0%	0%	0%	13%
More than \$60 million	6%	7%	2%	11%	18%	10%	6%	3%	18%	0%	0%	100%	10%	7%

Larger organizations are building out their AI teams

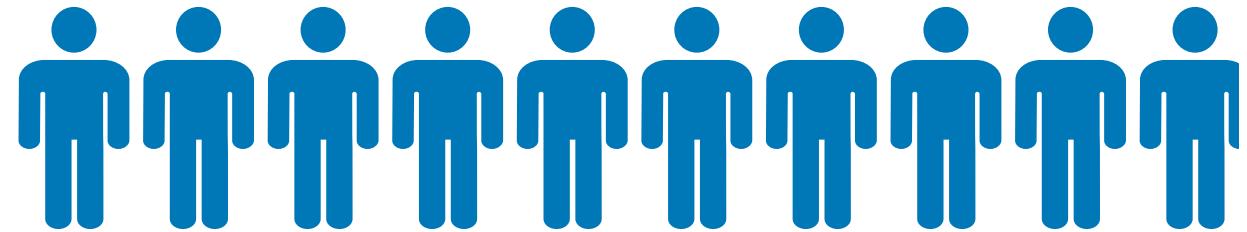
When asked about who the most senior AI governance employee is in the organization, certain roles stand out; the C-suite is generally correlated with less mature AI governance programs and seems to be the default for organizations starting out with AI governance. More mature organizations seem to settle on a senior vice president, vice president or a senior manager. While the survey data does not explain this divergence, the case studies seem to suggest hiring a manager with management skills from another digital governance discipline, such as privacy or data management, is a common path toward starting a successful AI governance program.

Organizations with less than USD100 billion in annual revenue are more likely to have their AI governance function report to the CEO or CFO. Higher-revenue organizations are more likely to be overrepresented in subpopulations, in which the AI governance function reports to the chief information officer, chief product officer, CISO or general counsel/head of legal. Medium- or high-revenue organizations rely on a variety of different executives. Alternatively, smaller organizations by revenue could have AI governance programs that use regular reporting structures and hierarchies to govern AI and are well integrated into their structures due to size.

Organization's revenue by AI governance staffing and needs

ORGANIZATION'S ANNUAL REVENUE IN USD	PEOPLE TASKED WITH AI GOVERNANCE								PEOPLE NEEDED FOR AI GOVERNANCE IN THE NEXT YEAR								
	Overall	1-10	11-20	21-30	31-40	41-50	51-75	100	0	1-10	11-20	21-30	31-40	41-50	51-75	76-100	>100
Less than \$100 million	20%	17%	2%	10%	0%	0%	0%	0%	30%	21%	4%	0%	0%	15%	0%	0%	0%
\$101-\$999 million	26%	28%	9%	10%	0%	20%	13%	0%	10%	29%	21%	7%	0%	8%	0%	0%	0%
\$1-\$8.9 billion	29%	31%	44%	40%	33%	0%	0%	0%	30%	30%	39%	47%	60%	15%	0%	0%	0%
\$9-\$19.9 billion	10%	11%	16%	20%	0%	0%	13%	33%	20%	9%	15%	20%	20%	15%	0%	40%	0%
\$20-\$59.9 billion	8%	7%	16%	10%	33%	40%	50%	33%	10%	7%	11%	20%	20%	15%	50%	20%	100%
More than \$60 million	6%	6%	13%	10%	33%	40%	25%	33%	0%	5%	10%	7%	0%	31%	50%	40%	0%

Organizations with between USD101 and USD999 million in annual revenue were overrepresented in the sample of organizations with one to 10 employees and underrepresented in the sample of organizations with 11-20 employees. The likelihood of an organization appearing in a sample of organizations with more than 21 employees increased significantly when the amount of revenue increased to more than USD1 billion.



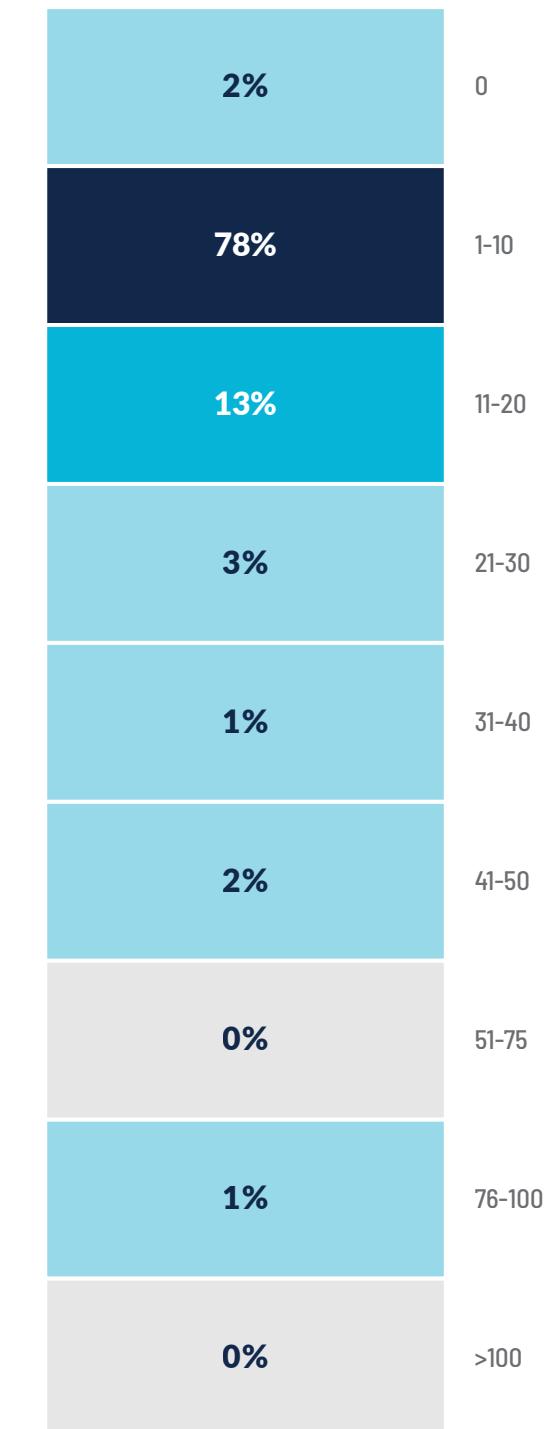
On average, organizations anticipate needing to task 9.8 people with AI governance over the next 12 months.

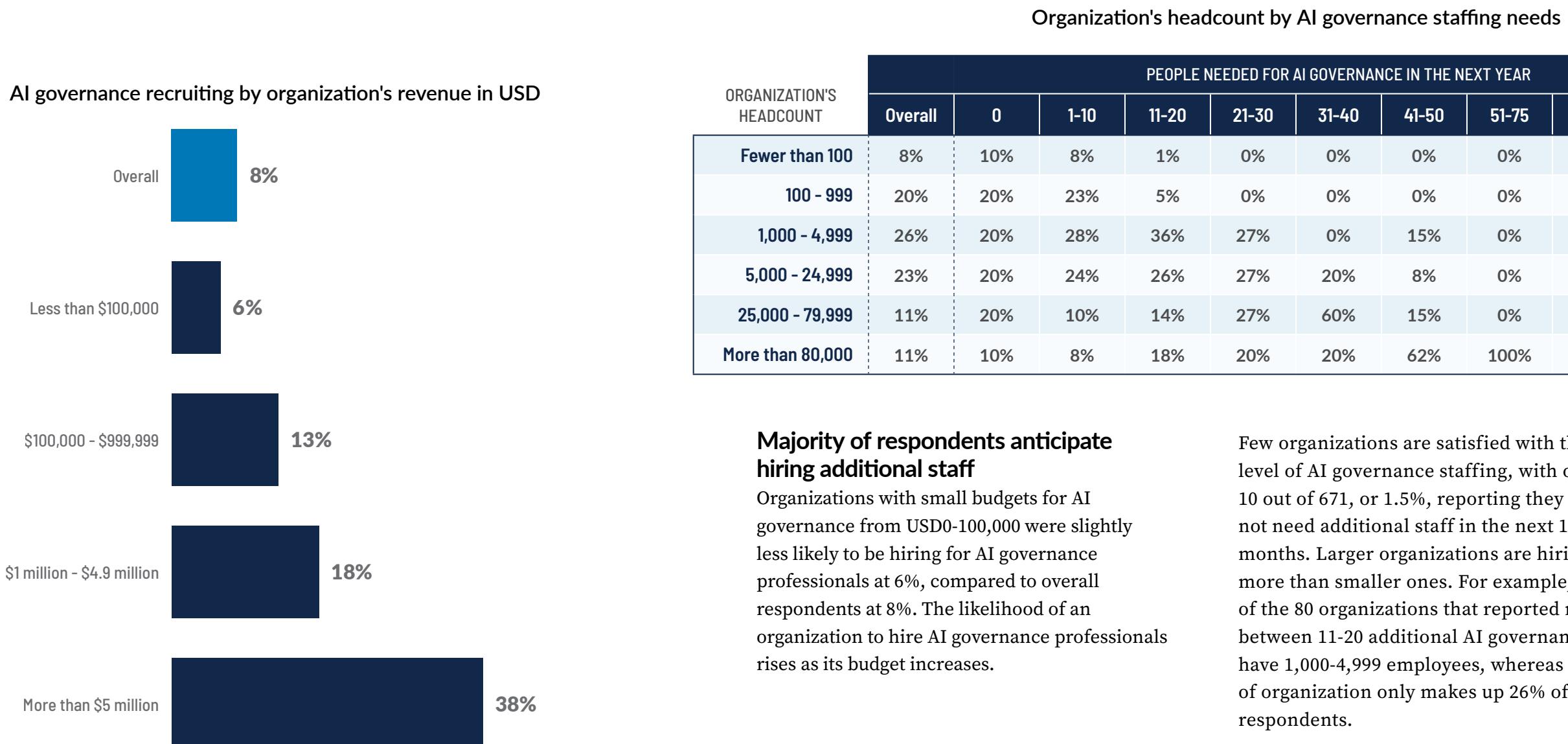
Organizations with between USD101 and USD999 million in annual revenue were overrepresented in the sample of organizations with one to 10 employees and underrepresented in the sample of organizations with 11-20 employees. The likelihood of an organization appearing in a sample of organizations with more than 21 employees increased significantly when the amount of revenue increased to more than USD1 billion.

The same is roughly true when it comes to the number of employees an organization is

looking to hire. Among those hiring one to 10 employees, organizations with less than USD100 million in annual revenue are overrepresented, while those with more than USD20 billion in annual revenue are underrepresented. The trend is reversed in the sample of organizations hiring 11-20 employees; those with less turnover are underrepresented in the sample. In the samples of organizations hiring more than 20 employees, there is sporadic overrepresentation of organizations with more than USD1 billion in annual revenue.

AI governance staffing needs





Case study: AI governance at Kroll



A global provider of financial and risk advisory solutions, Kroll is expanding its AI risk, governance and strategy services practice to meet the needs of its clients in an evolving and complex AI landscape. The company's AI Risk practice offers robust and comprehensive AI governance services and some insight into how to handle digital entropy across existing teams with diverse expertise.

While Kroll's AI Risk practice is designed to serve its clients, its team understands the importance of this internally as well. A working group of cross-functional professionals addresses AI risk and strategy for the firm, ensuring its practices are compliant and safe. Members of this cross-functional group include lawyers, product teams, sales and enablement functions, data scientists, computer and technical forensic experts, and privacy pros, who inform the solutions it delivers for clients. This coalition makes up the core AI governance team, which, in addition to considering the legal and regulatory implications of AI use, brings specialized technical experience to client solutions, including offensive security teams, red teaming, large language models and forensic experts looking at datasets that may include use of unauthorized IP.

The transformation and enhancement of Kroll's AI governance program is purpose-built to be a trusted advisor to its clients and the industry. Many of its clients are starting a similar journey in recognizing the necessity of technicians, data scientists and engineers for a

comprehensive governance program. This technical expertise complements existing legal and compliance professionals, ensuring a diverse set of capabilities can solve complex problems. As companies formalize their AI governance programs, a cross-functional set of interests and expertise often results in a committee or other governance structure overseeing AI use. This ensures AI governance is implemented in a way that accounts for different interests, strategies and risk thresholds across a company and accelerates thoughtful forward progress toward business objectives.

Tools that test and track AI use cases from ideation to deployment are being developed and deployed, including technology that can help illuminate, quantify and document regulatory risk while tracking compliance and mitigation requirements. These systems produce and collect documentation for relevant regulatory bodies and are vital to organizational success for Kroll and its clients.

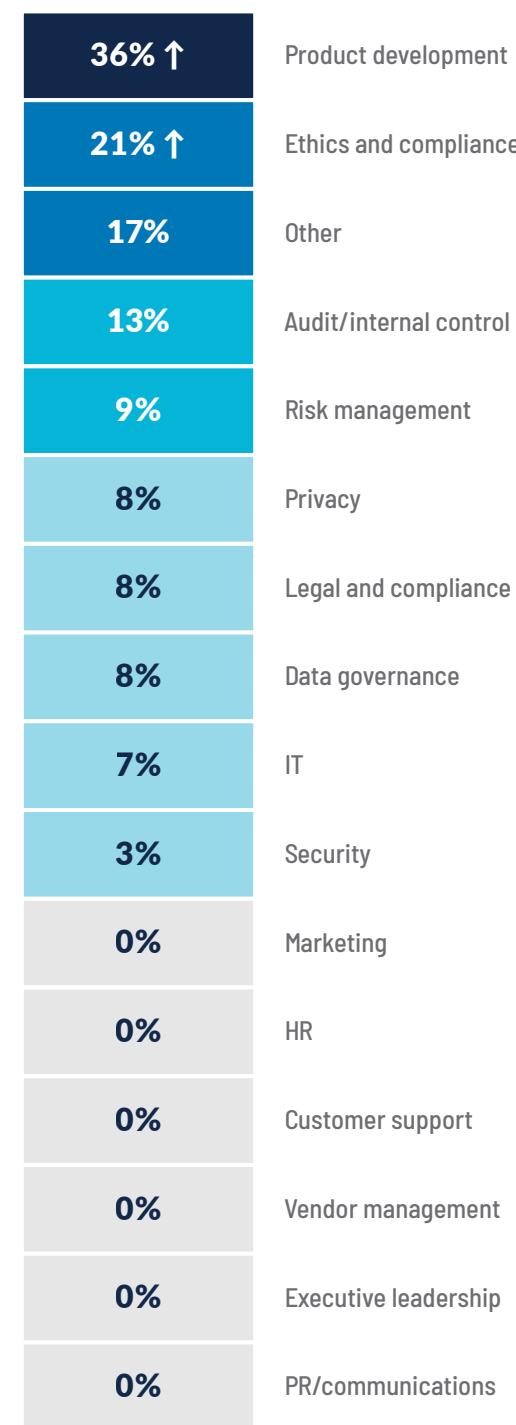
Product development and ethics and compliance functions hire AI governance professional

The case studies shed light on the skill sets needed on an AI governance team. The data shows several functions, such as IT, ethics, privacy, compliance and legal are commonly involved.

Organizations with their AI governance function in product development or ethics and compliance are more likely to hire AI governance professionals at 36% and 21%, respectively, than 8% of overall respondents. This could be due to the association of AI governance in product development with AI-focused companies or the association of ethics and compliance as the main AI governance function in large companies with mature AI governance programs.

AI governance was an interdisciplinary effort in case study companies. For smaller organizations, there will likely be less specialization but more upskilling for existing employees working in and across different adjacent roles.

AI governance recruitment by function within AI governance responsibility



Case study: AI governance at IBM

IBM has been at the forefront of AI technology for over a decade. Early on in their work, IBM researchers discovered risks associated with AI like bias and a lack of transparency. To mitigate those risks, company leadership saw the need to establish a strong foundation of AI governance.

The Chief Privacy Office was tasked with ensuring AI was developed and deployed in a responsible way. As that responsibility includes emerging technologies, the name was eventually changed to the Office of Privacy and Responsible Technology.

That office worked to augment the program originally built to track data privacy impact assessments, manage compliance with the GDPR, and incorporate AI and data governance so AI systems are developed and used in accordance with IBM policies.

The transformation necessitated a diverse team of experts from various fields. Technical specialists were crucial for adapting and maintaining the privacy and AI management system tool to meet evolving needs. Legal professionals played a vital role in examining existing and forthcoming laws, standards and regulations to guide the requirements for AI impact assessments and future compliance.

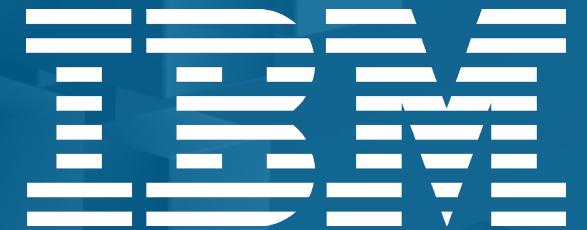
IBM also created the AI Ethics Board, the diverse and multidisciplinary team responsible for the governance and decision-making process for AI ethics policies and practices. It is charged with supporting a culture of ethical and responsible technology throughout the organization.

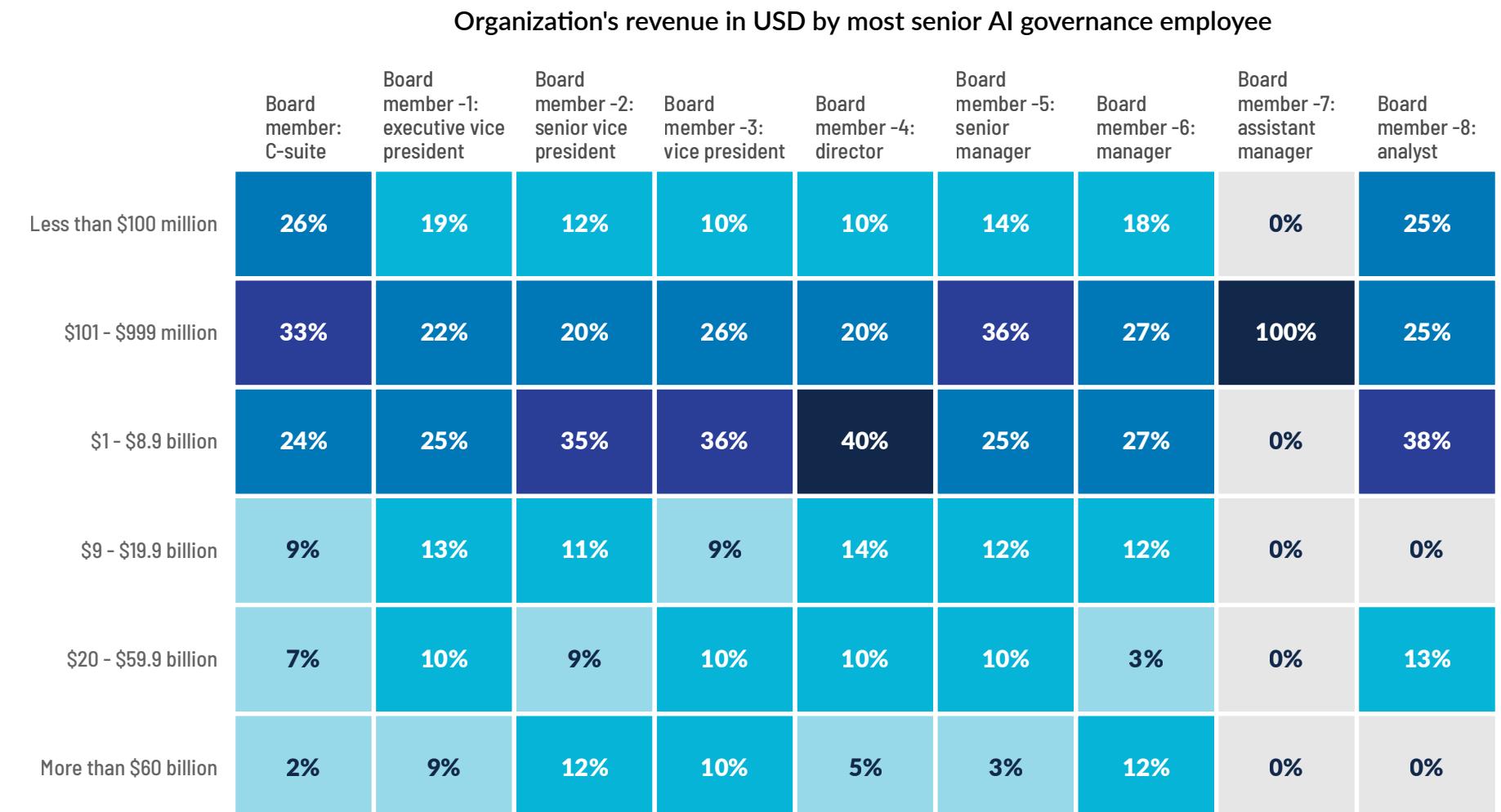
To balance the need for speed while maintaining strong AI governance, IBM established a core team of project managers and specialists with diverse backgrounds in technical software development, law and compliance within the Office of Privacy and Responsible Technology. Additionally, compliance specialists were established in the business units to assist in managing assessments and controls for new AI systems, based on identified risks.

Beyond the AI governance process, IBM employs communication and education specialists to ensure employee awareness of AI use policies and to disseminate information about AI governance

requirements across the organization. As AI technology advances and new applications emerge, the organization seeks to address evolving needs and maintain its position as a responsible AI developer and partner. For instance, as red teaming gains importance in AI governance, this skill set will be more in demand. While automation is crucial for scaling red teaming, human oversight remains essential.

As a global enterprise and technology innovator, IBM is well-positioned to tackle business challenges and create responsible AI governance capabilities. Operating in various geographies with diverse regulatory regimes requires a formalized, integrated system for managing AI governance efforts. Utilizing privacy compliance tools to manage AI governance facilitated a smooth transition for the core AI governance team and enabled the organization to sustain speed in the development and deployment of responsible AI.





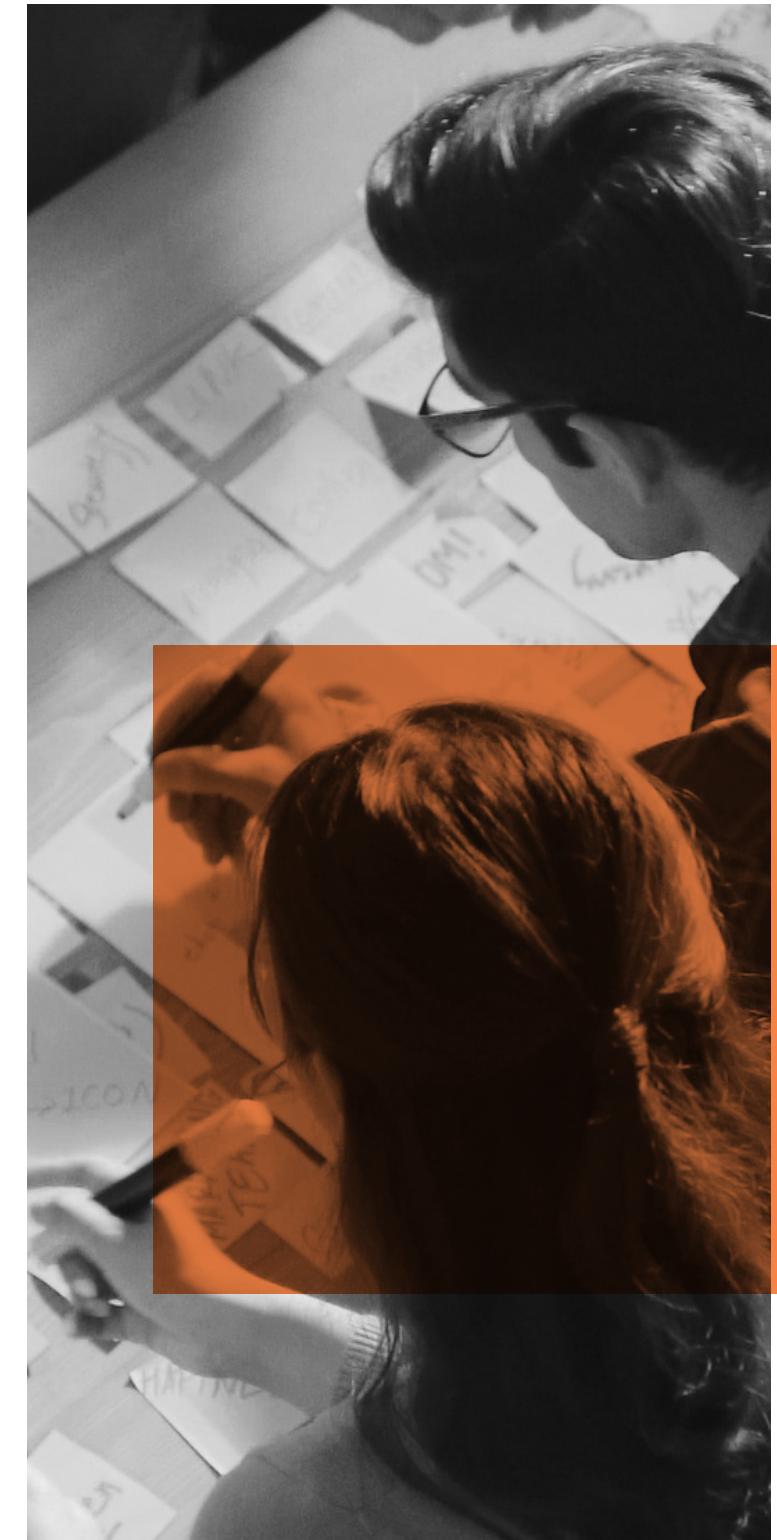
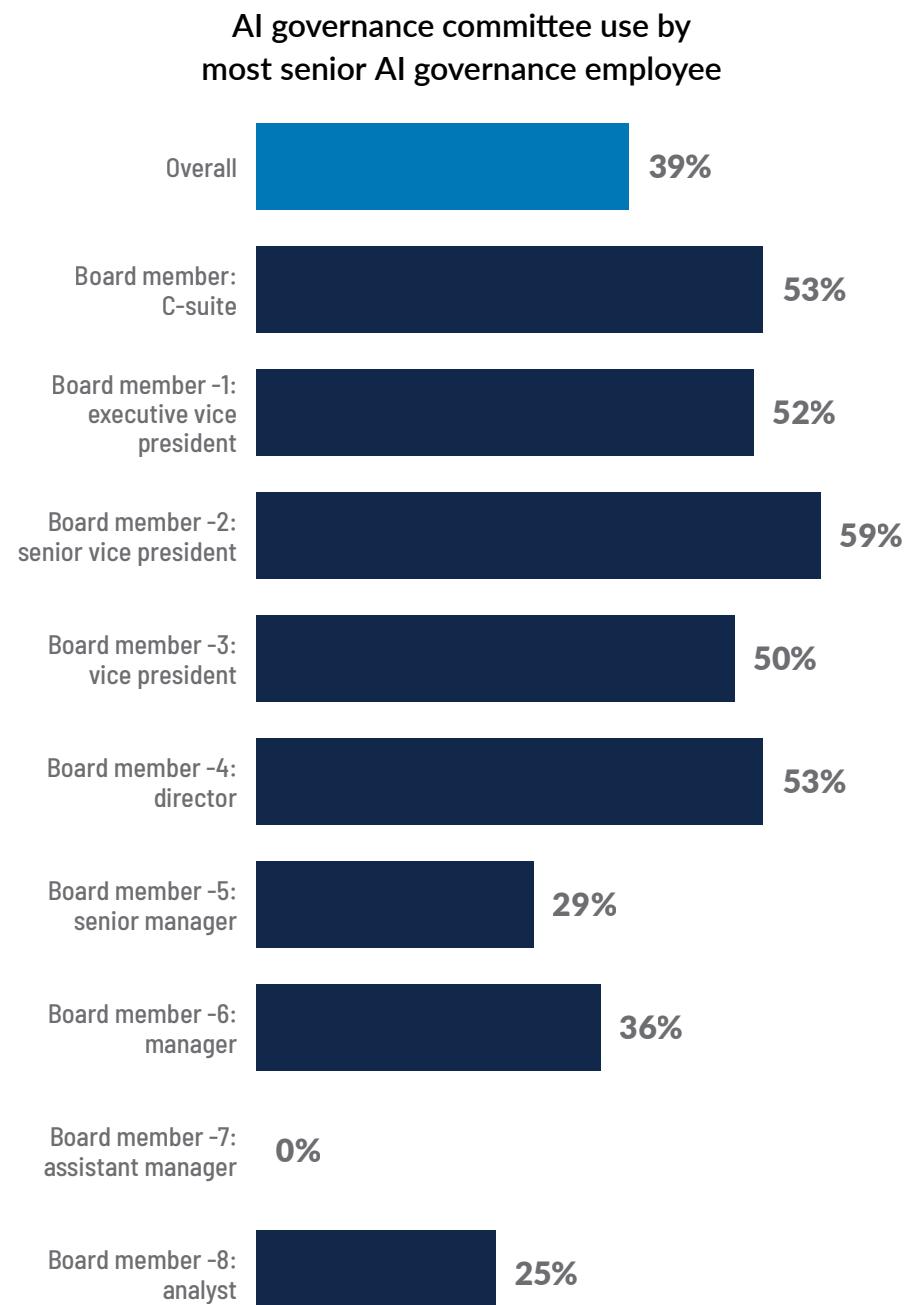
Senior vice presidents are more likely to lead AI governance at high revenue organizations

While 20% of organizations have an annual revenue of USD100 million, the number of organizations with someone in the C-suite

as the most senior AI governance employee is significantly higher at 26% and companies with more than USD1 billion annual revenue are much less likely to have a member of the C-suite as their most senior AI governance professional.

AI governance committees are more likely in companies when the senior most AI governance professional is a senior vice president

When looking at the intersection of the most senior AI governance employee and AI governance committee usage, approximately 39% of organizations have an AI governance committee. Organizations with a senior manager as the most senior AI governance employee are less likely to have an AI governance committee, at 29%. Those with a senior vice president as most senior AI governance employee are more likely to have an AI governance committee.

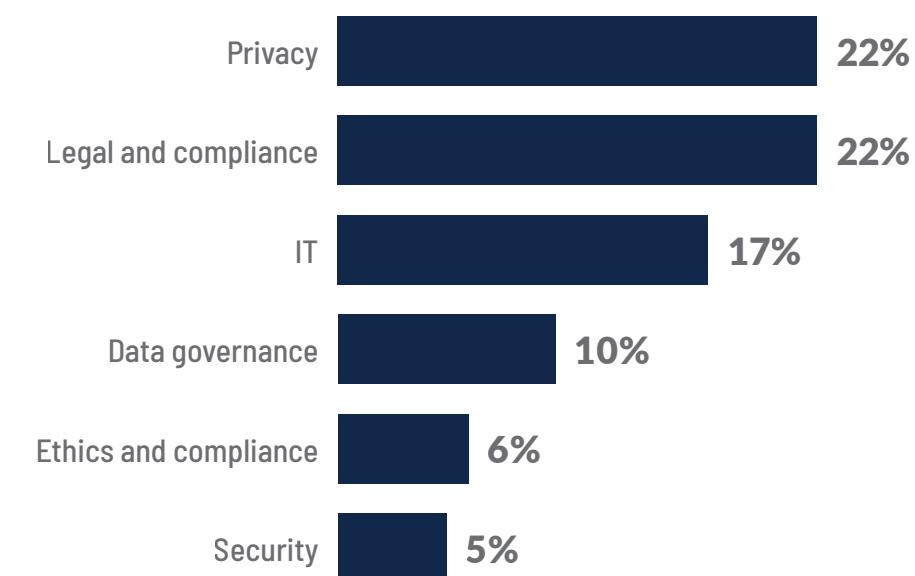


Part III. Leadership and accountability

Choosing the right leaders and holding them accountable is paramount for AI governance.

AI governance is usually seated within an existing department or team, and the data points to a few common options: IT, privacy, legal, compliance and others. HR and Marketing, however, were not chosen by any of the organizations to lead AI governance efforts. Many of the functions were also chosen to collaborate with the main function, giving evidence in favor of the hypothesis that AI governance is an interdisciplinary field. Who leads the efforts in the organization has a noticeable impact on AI governance efforts and is often correlated with different markers of AI governance maturity.

Top functions tasked with the primary responsibility for AI governance



Function with AI governance responsibility by AI use

FUNCTION WITH PRIMARY RESPONSIBILITY FOR AI GOVERNANCE	Overall	ORGANIZATION CURRENTLY USES AI FOR:								
		Process automation	Automated decision-making	Data analysis	Personalizing experiences	Customer interactions	Other	Not currently but expected to use AI within the next 12 months	Not currently using AI	Unsure
Privacy	22%	23%	21%	21%	24%	23%	21%	20%	19%	16%
Legal and compliance	22%	23%	26%	25%	24%	26%	33% ↑	14%	25%	8%
Security	5%	3%	4%	4%	5%	6%	5%	9%	0%	12%
IT	17%	13% ↓	10% ↓	13% ↓	11% ↓	10% ↓	14%	23%	28%	40% ↑
Data governance	10%	13%	12%	12%	9%	9%	5%	9%	6%	12%
Ethics and compliance	6%	8% ↑	10% ↑	7%	8%	8%	7%	5%	3%	0%

Organizations with AI governance functions in IT are less likely to use AI

Very few organizations have stand-alone departments specifically for responsible AI or AI governance. Several preexisting functions are utilized to take on responsibility for AI governance in the organization but there is no one-size-fits-all approach.

When asked about key challenges in reporting on AI governance, organizations with their AI governance function in IT overwhelmingly reported an absence of a clear mandate for AI governance at 21%, compared to only 17% of

overall respondents that have IT as the main AI governance function.

Organizations with AI governance functions in IT are less likely to use AI and more likely to be unsure about their AI use.

Data governance as the main function with responsibility for AI governance is correlated with a lower-than-average perceived shortage of AI governance professionals. IT does not see clarity in expectations, and ethics and compliance sees poor integration within broader risk management.



Function with AI governance responsibility by AI governance reporting challenges

FUNCTION WITH PRIMARY RESPONSIBILITY FOR AI GOVERNANCE	KEY CHALLENGES IN REPORTING ON AI GOVERNANCE									
	Overall	Lack of board-level understanding of AI	Lack of board-level understanding of AI governance	Absence of tangible metrics on AI governance	Absence of clear mandate for AI governance within the organization	Ineffective integration of AI governance with other complementary topics	Scope and objective of AI governance reporting not defined appropriately	Lack of maturity of AI governance within the organization hindering reporting to the board	AI risk management is yet to be fully established within the organization	Other
Privacy	22%	23%	22%	23%	22%	19%	22%	24%	22%	23%
Legal and compliance	22%	19%	21%	21%	18%	20%	22%	18%	19%	23%
Security	5%	4%	4%	5%	5%	3%	5%	5%	5%	7%
IT	17%	16%	13%	16%	21% ↑	15%	17%	16%	18%	23%
Data governance	10%	9%	12%	11%	11%	14%	10%	11%	12%	7%
Ethics and compliance	6%	7%	5%	7%	6%	7%	5%	6%	7%	7%

Function with AI governance responsibility by challenges delivering AI governance

FUNCTION WITH PRIMARY RESPONSIBILITY FOR AI GOVERNANCE	KEY CHALLENGES DELIVERING AI GOVERNANCE								
	Overall	Lack of understanding of AI and underling technologies	Lack of AI governance function representation in senior levels of organization	Organizational AI expectations are not clearly defined/followed up on	Lack of understanding within the organization of AI compliance governance obligations	Shortage of qualified AI professionals	Budget constraints	Not enough AI resources relative to the AI governance activities required to be completed	Competing priorities reducing focus on AI governance activities
Privacy	22%	20%	21%	18%	21%	24%	21%	22%	20%
Legal and compliance	22%	21%	21%	19%	21%	22%	25%	23%	25%
Security	5%	6%	4%	6%	5%	7%	7%	7%	6%
IT	17%	18%	16%	22% ↑	18%	17%	16%	15%	13%
Data governance	10%	12%	12%	11%	13%	5% ↓	11%	8%	8%
Ethics and compliance	6%	5%	7%	6%	7%	3%	5%	7%	6%

Case study: AI governance at Randstad

Randstad is a global talent company. It must take special care with its use of AI due to the increasingly regulated nature of AI use in the employment space.

For example, the EU AI Act considers AI systems used for recruitment or selection as high risk. The Colorado Act on Consumer Protections for AI similarly considers AI systems that make decisions around employment or employment opportunity as high risk. Randstad must also consider culturally diverse opinions about what is expected and acceptable in terms of AI use in the recruitment and employment processes given the diverse range of countries where it offers its services. These dual concerns lead to a unique approach to AI governance.

AI governance at Randstad is operated out of the joint legal and data protection department, in close cooperation with the data ethics function. As early as 2018, the legal and data protection department

was the first to spot the possible legal implications of using more advanced analytical and machine learning AI capabilities, and it in turn involved the IT department. These functions worked closely to define an initial set of AI principles in 2019; Randstad was one of the first companies to do so outside of the tech industry.

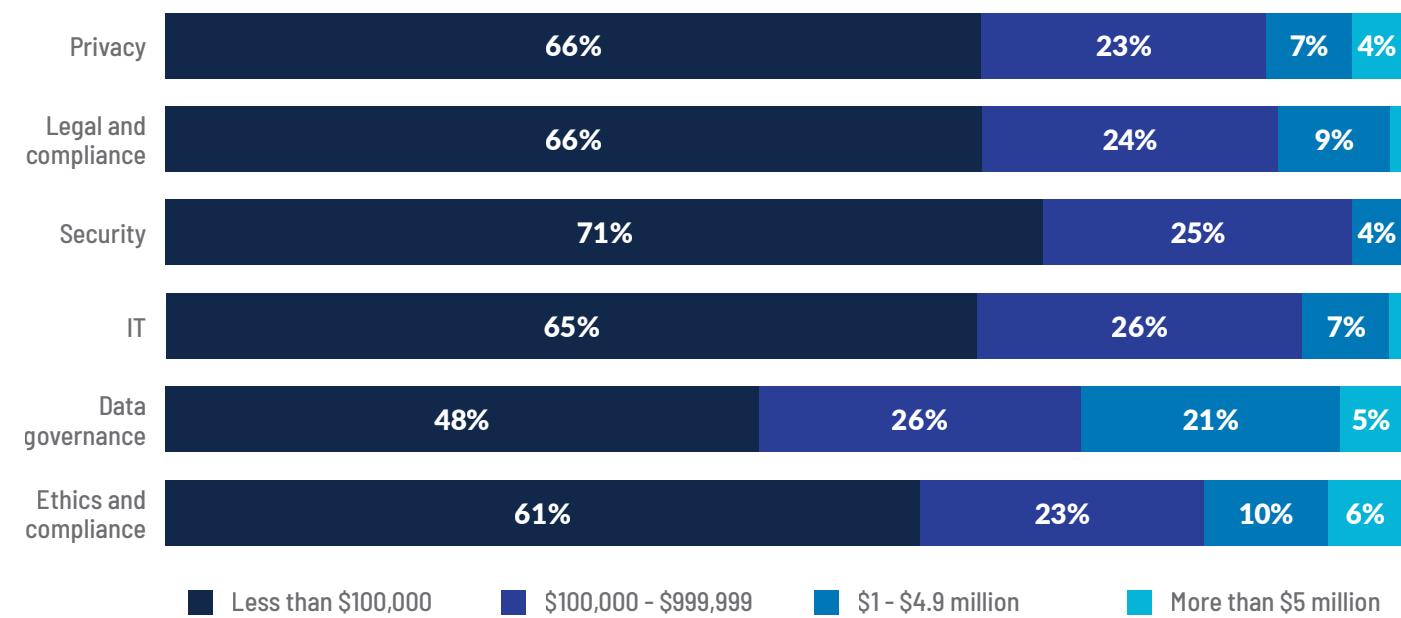
While Randstad does not have an independent AI governance function, it has freed up employees to play specific roles in AI governance, AI strategy and other AI-related roles. These core AI governance employees form a working group that handles the day-to-day operations. As its AI governance capabilities grow, the company has hired additional employees with specific skills. In the future, Randstad sees itself needing to

diversify its AI governance workforce geographically to bring in more perspectives.

Randstad maintains an AI steering committee for strategic direction and key decision-making around AI use. This committee also specifically looks at cross-border use cases, where there might be multiple legal jurisdictions as well as varying cultural values to consider. The steering committee also confirms any updates to Randstad's AI policy. Randstad also has a Data Ethics Advisory Board, which looks at ethical issues specifically. This board can work independently or under the behest of the AI steering committee as needs arise. Randstad sees value in having two distinct organs, so each can concentrate on its mission and be agile enough to make decisions quickly.



AI governance budget in USD by function with AI governance responsibility



Privacy and ethics and compliance are likely the better choice for leading AI governance

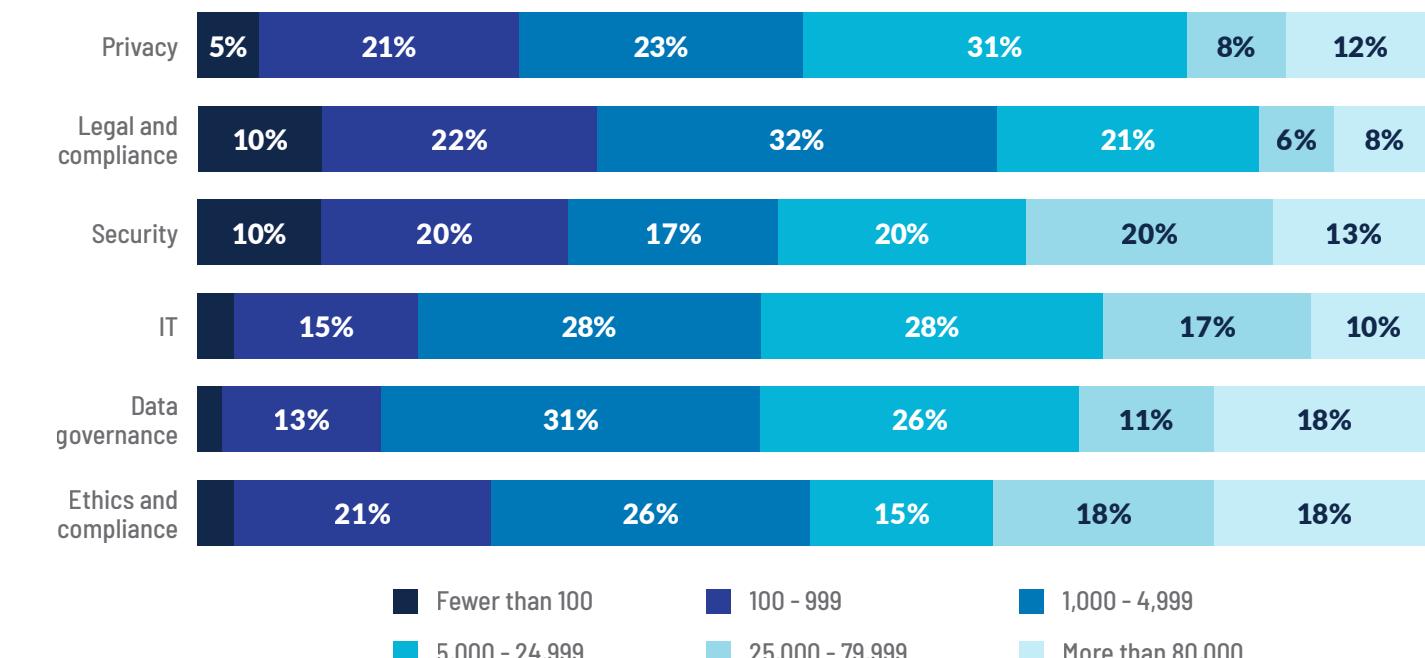
Many of the organizations in the case studies heavily relied on privacy or legal functions to build out their AI governance programs, and those functions ended up inheriting the responsibility. In the case above, the first department to bring it up as an issue to upper management became responsible. In the end, the work being done in AI governance is interdisciplinary in the skill sets involved, and this is reflected in the organization of the program. When talking to companies like Mastercard, it became clear a well-designed program will bring in experts from legal or IT as needed based on predefined requirements.

When asked about their level of confidence when it came to complying with the EU AI Act, 14% of respondents said they were "not at all confident" and 52% said they were either "somewhat confident" or "totally confident." When the primary responsibility for AI governance is with their organization's privacy function, respondents were significantly more likely to be confident in their ability to comply, at 67%. The same is true with ethics and compliance at 74%. IT was significantly less likely to be confident at 36%. Respondents working in audit/internal control were significantly more likely to respond "not confident at all" at 38%. This points to privacy and ethics and compliance as better candidates to have the main responsibility of AI governance and IT and audit/internal control as poor candidates.

When the primary responsibility for AI governance is with their organization's privacy function, respondents were significantly more likely to be confident in their ability to comply with the AI Act, at 67%.



Headcount by function with AI governance responsibility



Company size may determine which department is tasked with AI governance

While there still does not seem to be a strong pattern for size as a determinant of where an organization will seat AI governance, there are a few standouts, especially when looking at the average employee count among the different sample groups.

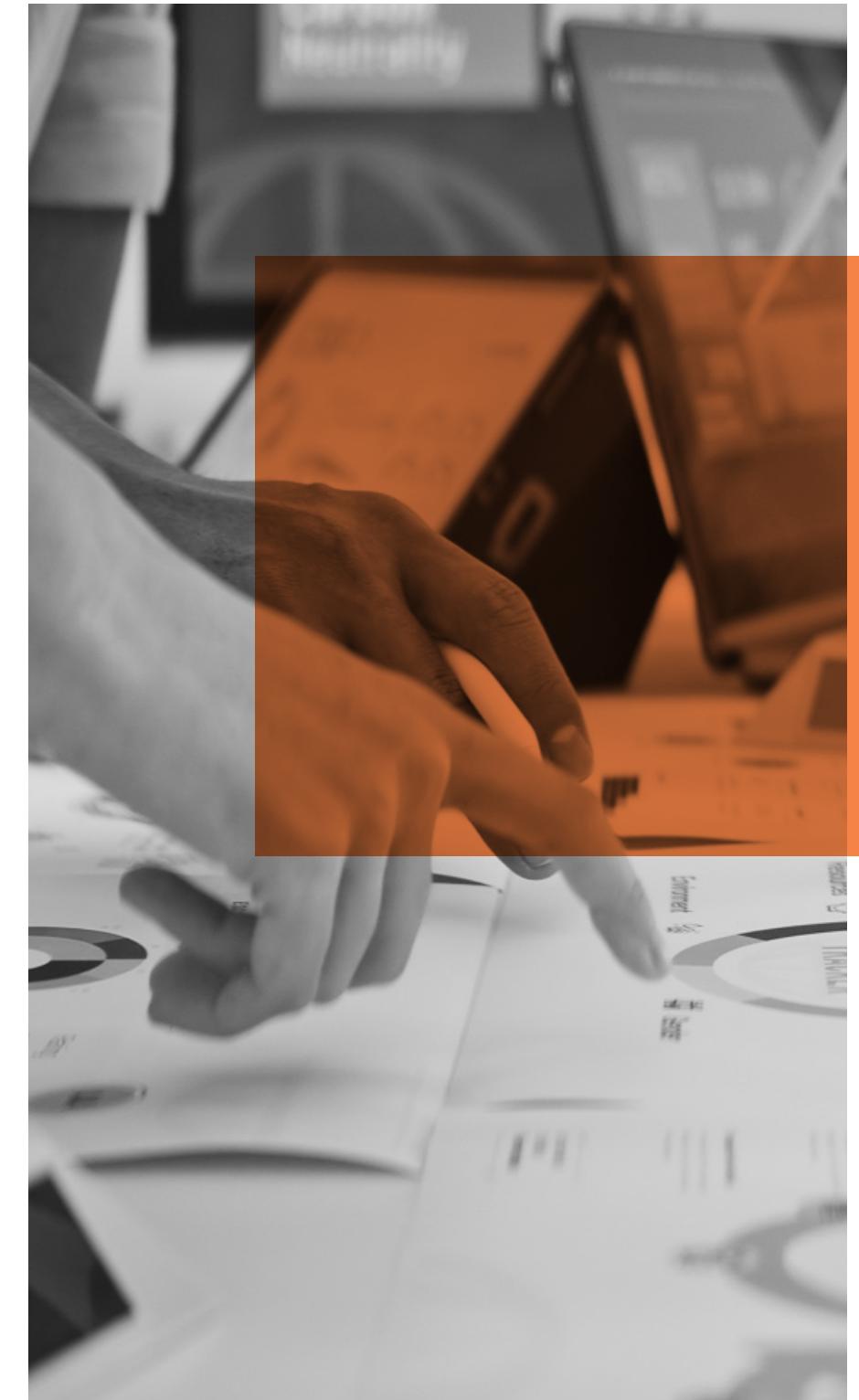
Whereas the average number of employees at respondents' organizations is 24,565 employees, the number of employees at companies where responsibility for AI governance is primarily delegated to ethics and compliance is significantly higher at 43,460 employees. Companies where respondents work in legal and compliance, on the other hand, have significantly fewer employees at 18,091 employees. This could point to larger companies having an ethics department and smaller companies combining this function with the legal department, while both still deal with compliance.

Most senior AI governance reporting by function with AI governance responsibility

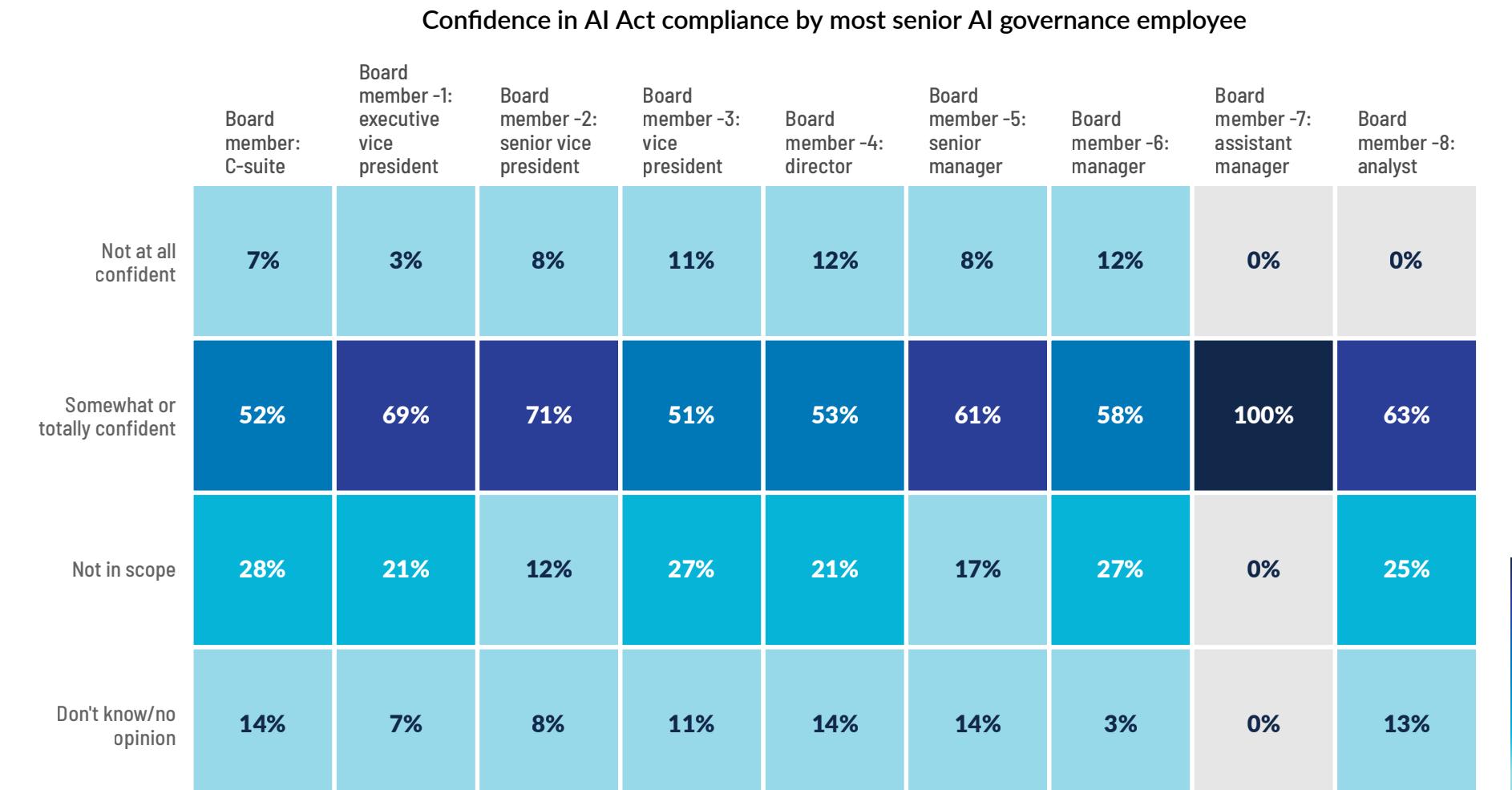
MOST SENIOR AI GOVERNANCE REPORTING	FUNCTION WITH PRIMARY RESPONSIBILITY FOR AI GOVERNANCE										
	Overall	Privacy	Legal and compliance	Security	Product development	IT	Data governance	Risk management	Executive leadership	Ethics and compliance	Other
General counsel/ head of legal	23%	34% ↑	56% ↑	4% ↓	8%	2% ↓	3% ↓	5% ↓	9%	26%	5% ↓
CEO	17%	13%	11%	25%	31%	11%	24%	14%	55% ↑	10%	23%
Chief compliance officer	7%	7%	8%	4%	8%	2%	9%	5%	5%	26% ↑	5%
COO	4%	4%	3%	0%	8%	6%	3%	5%	5%	3%	9%
Chief information officer	14%	6% ↓	3% ↓	8%	8%	43% ↑	17%	9%	9%	10%	9%
Chief technology officer	6%	4%	5%	8%	0%	10%	7%	5%	18% ↑	3%	0%
CISO	6%	10%	3%	29% ↑	0%	6%	3%	5%	0%	3%	0%
Chief risk officer	4%	3%	0% ↓	0%	8%	1%	9%	36% ↑	0%	3%	9%
CFO	3%	4%	4%	4%	0%	6%	0%	5%	0%	3%	0%
Chief people officer/ head of HR	0%	0%	0%	0%	0%	1% ↑	0%	0%	0%	0%	0%
Chief consumer officer/ head of customer	0%	0%	1%	0%	0%	0%	0%	0%	0%	0%	0%
Chief product officer	2%	1%	1%	0%	23% ↑	0%	2%	0%	0%	10% ↑	5%
Other	13%	15%	5% ↓	17%	8%	12%	22% ↑	14%	0%	3%	36% ↑

The disparity between these groups can also be seen in the previous figure, with legal and compliance more likely to report to the head of legal, while ethics and compliance is just as

likely to report to the head of legal or the chief compliance officer. This could also likely be explained by larger organizations having more specialization within their corporate structures.



When asked about confidence in their organization's ability to comply with the AI Act, respondents in organizations with a senior vice president as the most senior AI governance professional were the most likely to answer somewhat confident or totally confident at 71%.



When asked about confidence in their organization's ability to comply with the AI Act, respondents in organizations with a senior vice president as the most senior AI governance professional were the most likely to answer somewhat confident or totally confident at 71%,

compared to overall respondents at 52%. Those in organizations with a senior vice president as the most senior AI governance professional were also the least likely to say compliance with the AI Act was not in scope at 12% compared to the overall rate of 23%.

Most senior AI governance employee by function with additional AI governance responsibility

MOST SENIOR AI GOVERNANCE EMPLOYEE	FUNCTION WITH ADDITIONAL RESPONSIBILITY FOR AI GOVERNANCE																	
	Overall	Privacy	Legal and compliance	Security	Product development	Marketing	HR	Customer support	IT	Data governance	Risk management	Vendor management	Executive leadership	PR/communications	Audit/internal control	Ethics and compliance	Other	None
Board member: C-suite	11%	11%	11%	12%	8%	14%	16%	17%	10%	12%	13%	14%	13%	13%	11%	12%	13%	50% ↑
Board member -1: executive president	13%	10% ↓	13%	13%	16%	8%	13%	9%	14%	13%	12%	19% ↑	16%	13%	16%	16%	26%	17%
Board member -2: senior vice president	19%	20%	21%	21%	25% ↑	35% ↑	24%	37% ↑	21%	20%	23%	23%	25% ↑	28%	23%	22%	13%	0%
Board member -3: vice president	18%	19%	18%	19%	20%	19%	18%	13%	19%	16%	15%	16%	17%	15%	18%	14%	22%	33%
Board member -4: director	19%	21%	19%	20%	18%	12%	17%	11%	15% ↓	20%	19%	18%	13% ↓	15%	13% ↓	18%	4%	0%
Board member -5: senior manager	12%	12%	11%	8% ↓	6% ↓	5%	8%	7%	11%	11%	11%	6% ↓	8%	5%	12%	11%	17%	0%
Board member -6: manager	6%	6%	6%	5%	6%	5%	4%	6%	8%	6%	6%	2% ↓	5%	10%	5%	6%	4%	0%
Board member -7: assistant manager	0%	0%	0%	0%	1%	0%	0%	0%	0%	0%	0%	1%	0%	0%	0%	0%	0%	0%
Board member -8: analyst	2%	2%	2%	2%	1%	1%	1%	0%	0% ↓	2%	1%	2%	2%	3%	2%	1%	0%	0%

Organizations with a senior vice president as their most senior AI governance professional were the most likely to collaborate with other functions on AI governance, either

by the average likelihood to involve other departments or by how often they have statistically significant positive correlations with working with additional functions.

Most senior AI governance employee by function with additional AI governance responsibility

MOST SENIOR AI GOVERNANCE EMPLOYEE	FUNCTION WITH ADDITIONAL RESPONSIBILITY FOR AI GOVERNANCE																	
	Overall	Privacy	Legal and compliance	Security	Product development	Marketing	HR	Customer support	IT	Data governance	Risk management	Vendor management	Executive leadership	PR/communications	Audit/internal control	Ethics and compliance	Other	None
General counsel/head of legal	23%	21%	15% ↓	28% ↑	32% ↑	19%	20%	30%	25%	22%	20%	28%	26%	18%	21%	24%	17%	17%
CEO	17%	17%	18%	16%	18%	27% ↑	21%	20%	20% ↑	15%	16%	16%	20%	23%	16%	15%	30%	0%
Chief compliance officer	7%	8%	7%	6%	6%	4%	5%	5%	8%	8%	7%	5%	6%	3%	8%	7%	0%	0%
COO	4%	4%	5%	5%	2%	0%	3%	0%	5%	7% ↑	6%	5%	5%	0%	4%	5%	4%	0%
Chief information officer	14%	17% ↑	18% ↑	14%	7% ↓	14%	19% ↑	11%	9% ↓	16%	14%	13%	15%	20%	18%	18% ↑	9%	0%
Chief technology officer	6%	8% ↑	7%	6%	7%	4%	4%	4%	6%	7%	6%	8%	3% ↓	10%	8%	6%	0%	0%
CISO	6%	5%	6%	5%	4%	9%	8%	7%	5%	6%	7%	5%	4%	5%	6%	6%	0%	0%
Chief risk officer	4%	5%	6%	3%	4%	4%	3%	4%	5%	3%	4%	2%	3%	3%	4%	5%	0%	0%
CFO	3%	2% ↓	3%	3%	4%	4%	4%	5%	3%	3%	3%	4%	4%	0%	3%	3%	0%	33% ↑
Chief people officer/head of HR	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Chief consumer officer/head of customer	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	1%	0%	0%	0%	0%	0%	0%
Chief product officer	2%	2%	2%	2%	2%	3%	1%	0%	2%	3%	2%	1%	1%	0%	1%	0% ↓	0%	17% ↑
Other	13%	13%	13%	11%	14%	12%	12%	14%	12%	11%	15%	10%	12%	20%	12%	12%	39% ↑	33%

AI governance reporting follows linear lines of command, where the executive is reported to by its own departments
The organization's choice of which function is primarily responsible for AI governance likely determines who the most senior AI governance employee eventually reports to. While not

surprising, this also likely impacts which function ends up taking up the responsibility. For example, Randstad saw a change in executive leadership when the old chief technology officer left, and the program became less focused in the IT department and slowly moved over to the privacy and compliance function.

When comparing which function has the primary responsibility for AI governance with to whom the most senior AI governance employee reports, some obvious patterns emerge. The CEO, chief information officer and general counsel/head of legal were the most popular choices among the respondents at 17%, 14% and 23% respectively. Respondents at companies that sat AI governance with privacy said they were more likely to report to the general counsel/head of legal at 34% and less likely to report to the chief information officer at 6%. Legal and compliance was similarly more correlated with general counsel at 56% and less correlated with the chief information officer at 3%.

Respondents at the 24 organizations that tasked the security function with AI governance, on the other hand, were less likely to report to the general counsel/head of legal at 4% and more likely to report to the CISO at 29%, compared to overall respondents at 6%. IT was more correlated with reporting to the chief information officer at 43% and less correlated with reporting to general counsel/head of legal at 2%.



**The CEO, chief information officer and
general counsel/head of legal
were the most popular choices
for whom the most senior AI
governance employee reports to.**

Function with AI governance responsibility by whom the most senior AI governance employee reports to

FUNCTION WITH AI GOVERNANCE RESPONSIBILITY	Overall	MOST SENIOR AI GOVERNANCE EMPLOYEE ULTIMATELY REPORTS TO												
		General counsel/head of legal	CEO	Chief compliance officer	COO	Chief information officer	Chief technology officer	CISO	Chief risk officer	CFO	Chief people officer/head of HR	Chief consumer officer/head of customer	Chief product officer	Other
Privacy	22%	31% ↑	16%	22%	23%	10% ↓	13%	35%	14%	24%	0%	0%	10%	25%
Legal and compliance	22%	51% ↑	14%	24%	14%	4% ↓	19%	10%	0% ↓	24%	0%	100%	10%	9% ↓
Security	5%	1% ↓	7%	3%	0%	3%	6%	23% ↑	0%	6%	0%	0%	0%	6%
IT	17%	2% ↓	10%	5%	23%	51% ↑	26%	16%	5%	29%	100%	0%	0%	15%
Data governance	10%	2% ↓	16%	14%	9%	14%	13%	6%	23%	0%	0%	0%	10%	19% ↑
Risk management	4%	1% ↓	3%	3%	5%	3%	3%	3%	36% ↑	6%	0%	0%	0%	4%
Executive leadership	4%	2%	14% ↑	3%	5%	3%	13% ↑	0%	0%	0%	0%	0%	0%	0%
Ethics and compliance	6%	7%	3%	22% ↑	5%	4%	3%	3%	5%	6%	0%	0%	30% ↑	1%
Other	4%	1% ↓	6%	3%	9%	3%	0%	0%	9%	0%	0%	0%	10%	0% ↑

Risk management was less correlated with reporting to the general counsel/head of legal at 5% and more correlated with the chief risk officer at 36%, compared to overall respondents at 4%. Executive leadership was most likely to report to the CEO at 55% but also more likely to report to the chief technology officer at 18% compared to 6% of overall respondents. The ethics and compliance function was more likely to report to

the chief compliance officer at 25% compared to overall respondents at 7%.

While the data confirms the fact that reporting tends to follow the chain of command from whomever is chosen to take the helm with AI governance, the inverse, where the executive chooses the easiest home for AI governance that they control, also likely rings true.

Case study: AI governance at Cohere

Cohere is a growing startup that builds enterprise-grade frontier AI models and products designed to solve real-world business challenges.



Cohere's AI governance efforts are led by the multidisciplinary Responsible Machine Learning team, which combines both technical and nontechnical expertise. The Responsible ML team is deeply embedded throughout the organization, allowing direct feedback to travel between the team and the relevant functions represented on the team, like product or safety modeling.

Leading technical experts in safety modeling, AI security and data preprocessing are actively engaged in developing the state of the art in their fields, including by developing critical guidance and industry standards for responsible AI via industry groups and standards development organizations such as the U.S. National Institute of Standards and Technology, the Coalition for Secure AI and Open World Application Security Project. Legal and policy professionals within the Responsible ML team help connect the technical state of the art to evolving regulatory and customer

expectations, while product and compliance professionals within the team embed controls and standards into Cohere's products and processes.

Cohere delivers practical AI solutions for the enterprise market. It prioritizes flexible and secure deployment options, such as fully private deployments where customers can run AI models on premise or in their own virtual private clouds without access to customer data or computing environments. This means the AI governance efforts are centered on building safe and secure models that function robustly when faced with multilingual and cross-cultural applications, as well as real-world risks like cybersecurity, misinformation and bias.

It is important for downstream actors in the AI value chain, including Cohere's customers, to implement their own AI

governance guardrails, such as appropriate assessments and evaluation processes after Cohere models have been fine-tuned, customized or integrated into a customer AI system. For example, as detailed in Cohere's Enterprise Guide to AI Safety, bias risk can be introduced at any point in a model life cycle, including at the fine-tuning or deployment stage.

Looking ahead, two of the organization's key AI governance priorities in the next year will be to publish its Safety Framework, in line with voluntary commitments such as the Canadian Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems, U.K. Frontier AI Safety Commitments and Seoul AI Business Pledge, as well as continue its active contribution to the development of the Code of Practice for general-purpose AI model developers under the EU AI Act.

Headcount by whom the most senior AI governance employee reports to

ORGANIZATION'S HEADCOUNT	MOST SENIOR AI GOVERNANCE EMPLOYEE ULTIMATELY REPORTS TO													
	Overall	General counsel/head of legal	CEO	Chief compliance officer	COO	Chief information officer	Chief technology officer	CISO	Chief risk officer	CFO	Chief people officer/head of HR	Chief consumer officer/head of customer	Chief product officer	Other
Fewer than 100	8%	2%	14%	3%	5%	1%	0%	6%	5%	0%	0%	0%	10%	7%
100-999	20%	20%	32%	11%	14%	4%	3%	16%	9%	41%	0%	0%	30%	10%
1,000-4,999	26%	35%	29%	19%	36%	31%	32%	16%	18%	29%	100%	0%	10%	24%
5,000-24,999	23%	21%	10%	27%	23%	39%	26%	35%	23%	24%	0%	0%	30%	25%
25,000-79,999	11%	14%	3%	16%	9%	17%	23%	19%	14%	0%	0%	0%	10%	15%
More than 80,000	11%	8%	11%	24%	14%	7%	16%	6%	32%	6%	0%	100%	10%	19%

Smaller companies' AI governance functions are more likely to report to the CFO or CEO

While people working at organizations with 100-999 employees make up 20% of respondents, they make up 41% and 32% of those whose most senior AI governance professional ultimately reports to the CFO or CEO, respectively. Other medium or large companies are more likely to be overrepresented in samples whose most senior AI governance professional reports to the general counsel/head of legal, chief information officer,

chief technology officer or chief risk officer. This is also reflected in the average number of employees for each grouping of companies. The average number of employees for organizations who said the senior AI governance professional at their company reports to the CEO was significantly lower than overall respondents, and the opposite was true for the other reporting lines mentioned. Reporting to the CEO/CFO is something smaller organizations are likely to do, but different reporting lines are often chosen in organizations with more complex organizational structures.

Several functions will increasingly collaborate on AI governance

Generally, lack of cooperation among functions is not a significant issue for companies pursuing AI governance. AI governance is necessarily inter- and multidisciplinary. Nevertheless, there are benefits for companies that prioritize cross-functional collaboration, and these companies are also more likely to be more mature in their AI governance use.

There are several standout functions that respondents said will see additional involvement in AI governance programs: privacy at 57%, legal and compliance at 55%, security at 53%, IT at 52%, data governance at 44%, risk management

at 40%, executive leadership at 38%, and ethics and compliance at 35%. This excludes the number of organizations that already seat AI governance responsibility with those functions, so they are the most likely to be involved either as the principle or collaborative function.

There are a few standouts, such as organizations with executive leadership being more likely to collaborate with privacy at 83% and data governance at 65%. Respondents working in IT are more likely than overall respondents to collaborate with privacy at 72% and legal and compliance at 69%. Generally, most organizations plan to have cross-functional collaboration.

“

We have embedded responsible AI as part of our innovation process, and we are laser focused on AI literacy, so that we are AI-ready at all levels of our organization. We are also developing new tools and solutions to help others do the same, as we have a central role to play in connecting participants across the digital ecosystem. We look forward to working with partners in this space, so that together we can foster trust so that AI benefits everyone, everywhere.

Caroline Louveaux, CIPP/E, CIPM
Chief Privacy and Data Responsibility Officer at Mastercard

Functions with additional AI governance responsibility by function with AI governance responsibility

FUNCTIONS WITH ADDITIONAL AI GOVERNANCE RESPONSIBILITY	FUNCTION WITH PRIMARY RESPONSIBILITY FOR AI GOVERNANCE															
	Overall	None	Privacy	Legal and compliance	Security	Product development	Customer support	IT	Data governance	Risk management	Vendor management	Executive leadership	PR/communications	Audit/internal control	Ethics and compliance	Other
Privacy	57%	67%	0% ↓	66% ↑	70%	64%	0% ↓	72% ↑	82% ↑	70%	60%	83% ↑	100%	63%	88% ↑	75%
Legal and compliance	55%	83%	70% ↑	0% ↓	67%	36%	33%	69% ↑	76% ↑	61%	60%	74%	0%	75%	88% ↑	83% ↑
Security	53%	67%	62% ↑	55%	0% ↓	43%	0%	52%	55%	52%	60%	52%	0%	38%	65%	50%
Product development	25%	0%	30%	35% ↑	20%	0% ↓	0%	16% ↓	31%	9%	20%	22%	0%	13%	35%	17%
Marketing	13%	0%	16%	12%	13%	29%	33%	12%	11%	17%	20%	26%	0%	13%	6%	8%
HR	21%	17%	18%	15%	23%	21%	67% ↑	22%	27%	17%	40%	39% ↑	0%	25%	18%	21%
Customer support	10%	0%	10%	12%	13%	7%	0%	8%	15%	4%	40% ↑	13%	0%	38% ↑	3%	4%
IT	52%	50%	64% ↑	60% ↑	63%	50%	0%	0% ↓	79% ↑	52%	60%	65%	0%	50%	56%	63%
Data governance	44%	17%	46%	44%	43%	50%	100%	55% ↑	0% ↓	52%	40%	65% ↑	0%	63%	56%	46%
Risk management	40%	33%	40%	40%	43%	50%	0%	36%	58% ↑	0% ↓	20%	39%	0%	38%	38%	50%
Vendor management	24%	0%	27%	25%	30%	14%	33%	21%	23%	26%	0%	35%	0%	13%	18%	38%
Executive leadership	38%	0%	45%	37%	37%	50%	0%	38%	34%	48%	40%	0% ↓	0%	25%	47%	54%
PR/communications	7%	0%	8%	5%	10%	14%	0%	6%	6%	4%	20%	0%	0%	13%	6%	17%
Audit/internal control	25%	17%	28%	21%	23%	21%	0%	23%	37% ↑	26%	20%	17%	0%	0%	21%	33%
Ethics and compliance	35%	0%	38%	32%	33%	43%	0%	36%	42%	52%	40%	48%	0%	50%	0% ↓	42%

Functions with additional AI governance responsibility by challenges delivering AI governance

FUNCTIONS WITH ADDITIONAL AI GOVERNANCE RESPONSIBILITY	Overall	CHALLENGES DELIVERING AI GOVERNANCE							
		Lack of understanding of AI and underlying technologies	Lack of AI governance function representation in senior levels of the organization	Organizational AI expectations are not clearly defined/followed up on	Lack of understanding within the organization of AI compliance governance obligations	Shortage of qualified AI professionals	Budget constraints	Not enough AI resources relative to the AI governance activities required to be completed	Competing priorities reducing focus on AI governance activities
Privacy	57%	60%	65%	65%	62%	58%	63%	62%	61%
Legal and compliance	55%	56%	57%	62%	59%	56%	57%	59%	58%
Security	53%	57%	63% ↑	60%	62% ↑	61%	61%	63% ↑	59%
Product development	25%	27%	30%	24%	29%	26%	33% ↑	30%	33% ↑
Marketing	13%	14%	14%	16%	15%	16%	15%	13%	18%
HR	21%	24%	21%	23%	23%	23%	23%	23%	26%
Customer support	10%	12%	8%	9%	12%	9%	12%	10%	15% ↑
IT	52%	53%	56%	55%	57%	51%	57%	59% ↑	54%
Data governance	44%	45%	43%	49%	45%	49%	45%	47%	44%
Risk management	40%	45%	44%	45%	48% ↑	50% ↑	47%	49% ↑	47%
Vendor management	24%	27%	26%	26%	28%	28%	27%	28%	29%
Executive leadership	38%	41%	34% ↓	38%	40%	46%	46%	43%	47% ↑
PR/communications	7%	8%	6%	8%	9%	8%	8%	9%	12% ↑
Audit/internal control	25%	27%	32% ↑	25%	30%	28%	30%	30%	29%
Ethics and compliance	35%	40%	39%	36%	38%	44% ↑	37%	40%	32%
Other	4%	4%	4%	6%	6% ↑	4%	5%	5%	7%
None	2%	1%	1%	0%	1%	1%	0%	1%	3%

Organizations see collaboration with other departments as a way to shore up areas of challenges.

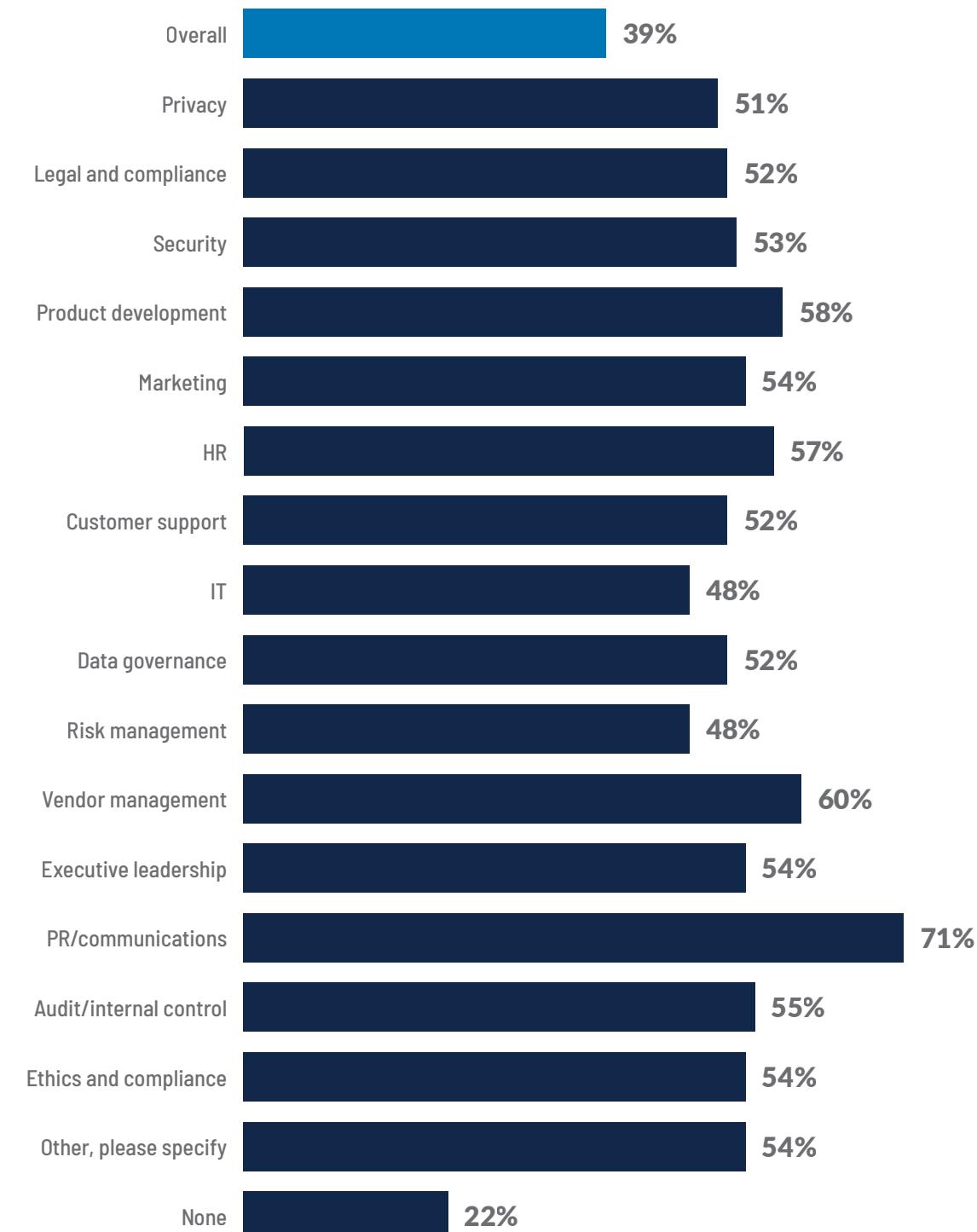
The data suggests organizations are properly targeting their AI governance programs based on their individual issues. Security appears to be one of the more likely to gain additional involvement when the organization has challenges, as it is overrepresented when there is a lack of AI governance representation, lack of understanding of AI governance compliance obligations and too few resources.

Functions with additional AI governance responsibility by AI governance reporting challenges

FUNCTIONS WITH ADDITIONAL AI GOVERNANCE RESPONSIBILITY	Overall	CHALLENGES REPORTING ON AI GOVERNANCE								
		Lack of board-level understanding of AI	Lack of board-level understanding of AI governance	Absence of tangible metrics on AI governance	Absence of clear mandate for AI governance within the organization	Ineffective integration of AI governance with other complementary topics	Scope and objective of AI governance reporting not defined appropriately	Lack of maturity of AI governance within the organization hindering reporting to the board	AI risk management is yet to be fully established within the organization	Other
Privacy	57%	58%	59%	57%	61%	66% ↑	65% ↑	61%	63%	60%
Legal and compliance	55%	58%	56%	60%	61%	61%	60%	61%	58%	60%
Security	53%	55%	56%	57%	61% ↑	57%	60%	61% ↑	61% ↑	47%
Product development	25%	27%	26%	29%	25%	28%	28%	27%	29%	40%
Marketing	13%	19%	21% ↑	14%	16%	16%	17%	17%	17% ↑	17%
HR	21%	22%	22%	23%	23%	28% ↑	24%	26% ↑	24%	20%
Customer support	10%	8%	12%	12%	10%	11%	12%	12%	13% ↑	10%
IT	52%	52%	55%	55%	54%	58%	59% ↑	59% ↑	59% ↑	50%
Data governance	44%	43%	48%	47%	44%	50%	48%	49%	46%	53%
Risk management	40%	48%	47%	43%	42%	46%	48% ↑	47% ↑	42%	33%
Vendor management	24%	25%	25%	26%	26%	28%	29%	29%	29%	37%
Executive leadership	38%	34%	38%	42%	41%	44%	43%	43%	47% ↑	30%
PR/communications	7%	8%	8%	8%	8%	9%	10%	8%	9%	7%
Audit/internal control	25%	29%	30%	27%	28%	29%	30%	32% ↑	26%	37%
Ethics and compliance	35%	34%	37%	38%	37%	45% ↑	40%	40%	38%	30%
Other	4%	2%	2%	4%	4%	4%	4%	5%	5%	13% ↑
None	2%	1%	1%	1%	1%	2%	0%	1%	1%	0%

Organizations anticipating or planning for cross-functional collaboration saw challenges in reporting on AI governance in risk management, maturity and reporting scope.

AI governance committee use by function with additional AI governance responsibility



Organizations with AI governance committees are also more likely to increase collaboration.

While 39% of respondents said their organizations have an AI governance committee, the rate was much higher among respondents who said their organizations were involving other functions in AI governance. This was significantly true for all functions except for customer support and risk management, although organizations involving these functions also had nominally higher AI governance committee rates than general respondents.

Organization's revenue by function with additional AI governance responsibility

ORGANIZATION'S ANNUAL REVENUE IN USD	FUNCTION THAT WILL HAVE ADDITIONAL INVOLVEMENT IN AI GOVERNANCE																	
	Overall	Privacy	Legal and compliance	Security	Product development	Marketing	HR	Customer support	IT	Data governance	Risk management	Vendor management	Executive leadership	PR/communications	Audit/internal control	Ethics and compliance	Other	None
Less than \$100 million	20%	14%	12%	14%	14%	19%	11%	23%	17%	10%	13%	15%	16%	7%	10%	8%	17%	44%
\$101-\$999 million	26%	25%	25%	25%	29%	23%	22%	16%	23%	23%	22%	22%	25%	10%	24%	19%	21%	22%
\$1-\$8.9 billion	29%	33%	32%	34%	30%	30%	33%	32%	32%	34%	36%	32%	33%	34%	34%	37%	38%	22%
\$9-\$19.9 billion	10%	10%	12%	12%	10%	10%	15%	11%	13%	13%	14%	11%	9%	17%	14%	16%	8%	11%
\$20-\$59.9 billion	8%	10%	11%	8%	7%	10%	10%	10%	8%	10%	8%	11%	8%	20%	11%	11%	8%	0%
More than \$60 billion	6%	8%	8%	7%	9%	9%	10%	8%	7%	10%	7%	10%	9%	12%	8%	10%	8%	0%

Higher revenue and larger organizations are looking to increase AI governance collaboration

While 20% of respondents said their organizations have an annual revenue of less than USD100 million, this group is overrepresented in the sample that answered none when asked about additional functions that will be involved in AI governance. They were significantly underrepresented in samples that said they would

involve privacy at 14%, legal and compliance at 12%, security at 14%, HR at 11%, data governance at 10%, risk management at 13%, audit/internal control at 10%, and ethics and compliance at 8%. This trend implies smaller organizations are less likely focus on cross-functional collaboration.

The same is true when comparing the number of employees to which functions will have additional responsibilities for AI governance.

Headcount by function with additional AI governance responsibility

ORGANIZATION'S HEADCOUNT	FUNCTION THAT WILL HAVE ADDITIONAL INVOLVEMENT IN AI GOVERNANCE																	
	Overall	Privacy	Legal and compliance	Security	Product development	Marketing	HR	Customer support	IT	Data governance	Risk management	Vendor management	Executive leadership	PR/communications	Audit/internal control	Ethics and compliance	Other	None
Fewer than 100	8%	5%	2%	4%	4%	5%	2%	10%	6%	3%	4%	1%	5%	5%	1%	2%	0%	11%
100-999	20%	16%	16%	17%	18%	19%	14%	16%	17%	14%	17%	15%	18%	7%	15%	12%	25%	44%
1,000-4,999	26%	29%	27%	31%	33%	29%	33%	31%	28%	27%	27%	33%	29%	22%	27%	26%	29%	22%
5,000-24,999	23%	24%	26%	24%	20%	21%	21%	19%	25%	26%	27%	26%	23%	22%	24%	26%	13%	22%
25,000-79,999	11%	14%	15%	12%	10%	14%	15%	11%	11%	15%	12%	11%	12%	24%	17%	19%	21%	0%
More than 80,000	11%	12%	13%	13%	15%	13%	15%	13%	14%	15%	14%	13%	13%	20%	16%	15%	13%	0%

Confidence in AI Act compliance by function with additional AI governance responsibility

CONFIDENCE IN ABILITY TO COMPLY WITH THE EU AI ACT	FUNCTION THAT WILL HAVE ADDITIONAL INVOLVEMENT IN AI GOVERNANCE																	
	Overall	Privacy	Legal and compliance	Security	Product development	Marketing	HR	Customer support	IT	Data governance	Risk management	Vendor management	Executive leadership	PR/communications	Audit/internal control	Ethics and compliance	Other	None
Not at all confident	14%	10%	7% ↓	10%	9%	8%	7%	6%	8% ↓	10%	11%	8%	8%	5%	9%	11%	13%	22%
Somewhat or totally confident	52%	54%	59%	59%	66% ↑	63%	68% ↑	68%	60% ↑	57%	57%	61%	60%	71%	62%	60%	42%	22% ↓
Not in scope	23%	22%	23%	22%	17%	18%	16%	18%	20%	22%	22%	24%	23%	17%	21%	19%	33%	33%
Don't know/no opinion	12%	14%	11%	10% ↓	9%	13%	9%	8%	12%	11%	11%	6% ↓	8% ↓	7%	8% ↓	11%	13%	22%

Certain collaborations have higher confidence in complying with AI Act

When asked about their organization's confidence in complying with the AI Act, 52% of respondents said they felt somewhat or totally confident in their ability to comply, while 14% said they did not feel confident at all. When asked which functions will be involved with AI governance, several responses were correlated with being more confident than general

respondents, such as product development at 66%, HR at 68% and IT at 60%. Those who did not expect any cross-functional collaboration were significantly less likely to feel confident in their ability to comply with the AI Act at 22%. Two functions, specifically legal and compliance at 7% and IT at 8%, were highly correlated with being less likely than overall respondents to say that they were not at all confident in compliance.

What makes a mature AI governance program?

AI governance is not a one-size-fits-all approach. As can be seen through the case studies, each organization ends up with a structure that fits its unique challenges and business model. For example, companies that are smaller will be less inclined to build out extensive teams and structures, while larger teams will find this valuable and necessary. This can explain some of the variance seen in team size and budget, where larger companies are more likely to have more formal, built-out AI governance programs.

Furthermore, organizations just starting to use AI internally might start slowly until they are ready to make a greater investment in an AI governance program. Organizations should look at their motivations for starting an AI governance program and use this as a jumping off point. Usually, organizations are motivated by a realization of a coming compliance burden, a desire to gain efficiencies through AI or market pressure. This should then inform the

organizational strategy around AI use, which should in turn inform organizational policy around AI governance.

When building out the AI governance program, the first place to look is the AI risk management process — a common theme throughout the case studies of organizations deploying AI. Through this process, the organization can first build an inventory of what AI systems are in place. Then, when new AI systems are ideated, these can be checked against potential risks and the organization's strategy. By using this as a filter for both risk and strategy management, organizations can prioritize use cases that provide the best risk-to-benefit ratio.

Building out a team with a good understanding of the risks and possibilities around AI use to manage this process and act as an advocate for AI internally is a good first step. While an external expert might be hired to run this program, oftentimes an existing employee in privacy or data management who is already familiar with data and privacy governance might be able to jump in.





The choices an organization makes should suit them and their circumstances, but the organization should nonetheless remain flexible as new guidance and compliance burdens appear.

The team members of a mature AI governance program will know when to bring in experts from a variety of disciplines. These might be from IT, privacy, compliance, ethics or legal departments, and efforts should be undertaken to upskill employees when necessary. These employees all work tangentially on AI issues already, so getting them up to speed will be relatively easy. Existing structures and processes should be adapted to avoid creating unnecessary new artifacts. As in many of the case study organizations, existing privacy impact assessments can be leveraged to include questions for AI risk assessments.

The choices each organization makes about the structures, processes and policies they choose to employ will have lasting effects. The choices an organization makes should suit them and their circumstances, but the organizations should nonetheless remain flexible as new guidance and compliance burdens appear. In the case studies, the companies benefitted from previous processes and structures they could adapt to use for AI governance. Anything that is implemented for AI governance today only eases future compliance and governance efforts.

Conclusion

Organizations are thinking seriously about how to best approach AI governance.

This report shows there is no one single path; each organization will need to consider its objectives and unique situation when deciding how to develop its AI governance program. While organizations can leverage their existing privacy and compliance functions to support AI governance, AI introduces unique risks that require collaboration across functions. There is a recognition of the unique risks related to AI systems that require expertise in areas such as computer science and model risk management. While many existing privacy and cybersecurity risks, such as model drift, confabulations or hallucinations, can be addressed with data governance and cybersecurity risk management, measuring the socio-technical risks of AI systems will require additional AI governance measures. Specificity, standards and benchmarks developed jointly by the academic community and AI practitioners from private industry and standard-setting bodies will be paramount to create a robust AI governance and AI assurance ecosystem. Other hallmarks of a mature AI governance program include having an oversight body and clear lines of communication, including reporting, internal AI literacy training and information dissemination throughout the organization.

The seven case studies highlight the diversity of approaches from large established global companies to young AI-focused companies. The companies are aware of and are preparing for their obligation to comply with regulations. Some commonalities emerged when comparing one case to the next, such as having a risk assessment and mitigation process. For many organizations, this process has become a central part of how they structure their approaches to cataloging, analyzing and ensuring compliance of their AI systems.

As more legislation regulating AI throughout the world emerges, organizations will likely feel more of a push to have a formal, structured approach to AI governance. However, emerging regulation is not the only impetus for businesses to establish their own AI governance programs. AI governance can also be a catalyst for enterprise growth, enhancing brand credibility and providing the certainty businesses need to manage a constantly evolving technological field and regulatory landscape. Identifying and addressing risks can enable business growth, especially in providing the ability to derisk a large amount of low-risk AI use cases with effective AI governance to consequently unblock areas of efficiency, creativity and innovation for enterprises of all sizes. Streamlining the ability to classify, categorize and appropriately address different use cases based on their level of risk enables enterprises to move faster with AI.

By understanding what similar organizations are doing, organizations can benchmark their own AI governance programs and not only adjust their own programs but add to the growing body of knowledge that informs the understanding of AI governance maturity. AI is a cutting-edge technology and AI governance is still an emerging field, which requires testing and evaluation of different methods, processes and standards over time. Sharing best practices and insights among enterprises will help to set precedents and create achievable yet meaningful benchmarks for companies seeking to effectively identify, manage and mitigate risks associated with their AI systems.





Contacts

Connect with the team

Richard Sentinella
IAPP AI Governance Center
Research Fellow
rsentinella@iapp.org

Evi Fuelle
Global Policy Director,
Credo AI
evi@credo.ai

Joe Jones
IAPP Director of Research
and Insights
jjones@iapp.org

Ashley Casovan
IAPP AI Governance Center
Managing Director
acasovan@iapp.org

Lynsey Burke
IAPP Research and Insights
Operations Manager
lburke@iapp.org

Follow the IAPP on social media



Published April 2025.

IAPP disclaims all warranties, expressed or implied, with respect to the contents of this document, including any warranties of accuracy, merchantability, or fitness for a particular purpose. Nothing herein should be construed as legal advice.

© 2025 IAPP. All rights reserved.