Gartner
Peer Community™

Generative AI Security and Risk Management Strategies

With growing interest in generative AI tools and foundational models among organizations and individuals alike, IT and security leaders are challenged to mitigate the accompanying risks of this rapidly developing tech. Given the emergent nature and deep complexity of this area, what strategies are these leaders turning to so far?

One-Minute Insights:

- Almost all respondents say their organization is currently using, planning to use or considering generative AI
- Over one-third are already using or implementing AI application security tools
- Most surveyed IT/security leaders report their organization's generative AI security and risk management strategy involves the formation of new working groups
- Many say their organization is facing team or skills gaps in its generative AI security/risk management efforts
- Incorrect/biased outputs and insecure code are among the generative AI risks that respondents are most concerned about for their organization

One-Minute Insights on timely topics are available to Gartner Peer Community members. Sign up for access to over 100 more, and new insights each week.

Data collection: Apr 1 - Apr 7, 2023

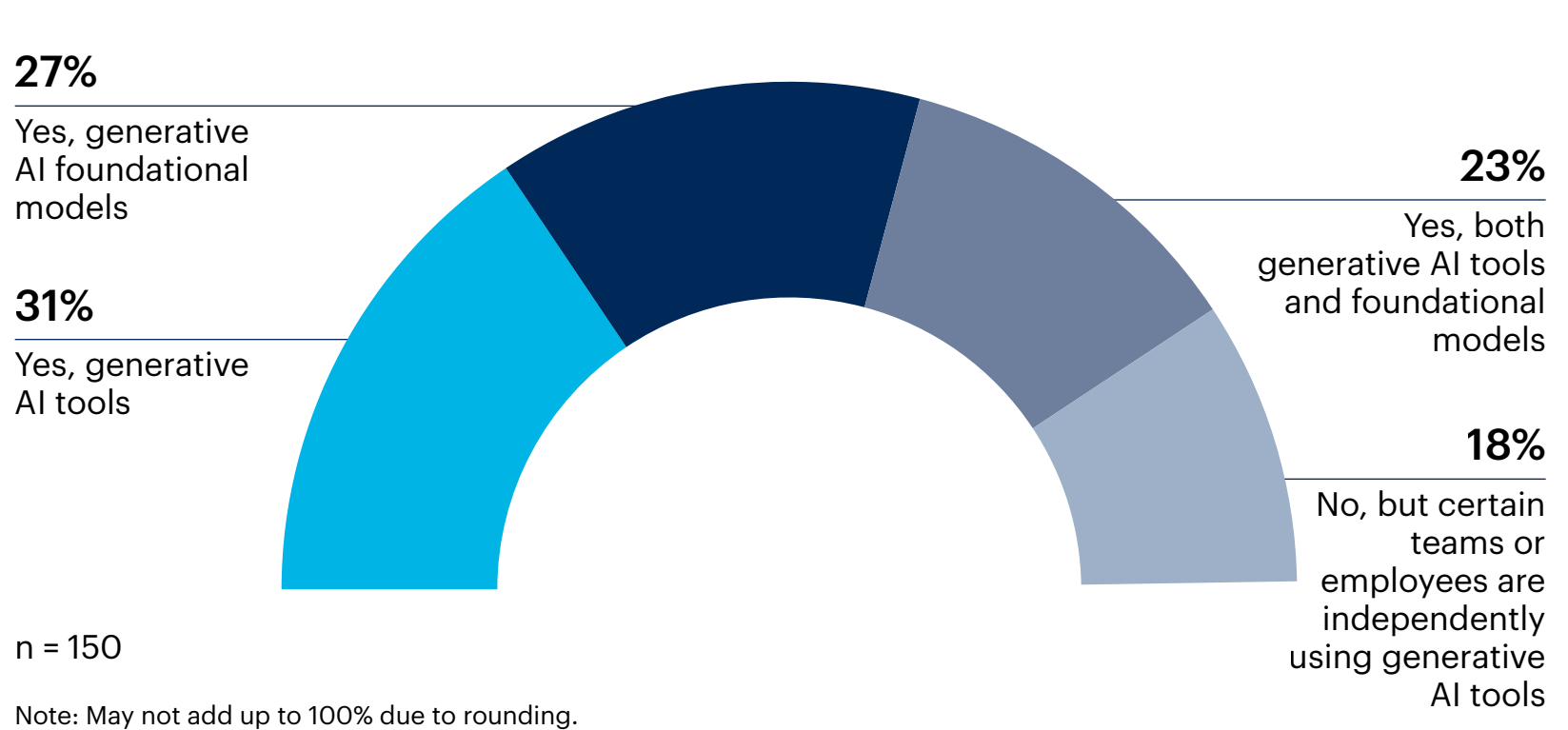
Respondents: 150 IT and information security leaders at organizations where generative AI or foundational models are in use, in plans for use, or being explored

Most say their organizations are using or considering generative AI and that IT is responsible for related security and risk management efforts

Respondents report that their organization is exploring, using or planning to use either generative AI tools (31%), foundational models (27%) or both (23%).

Almost one-fifth (18%) of respondents say certain employees or teams at their organization are using these tools independently.

Is your company currently using, planning to use, or exploring generative AI tools or foundational models?*



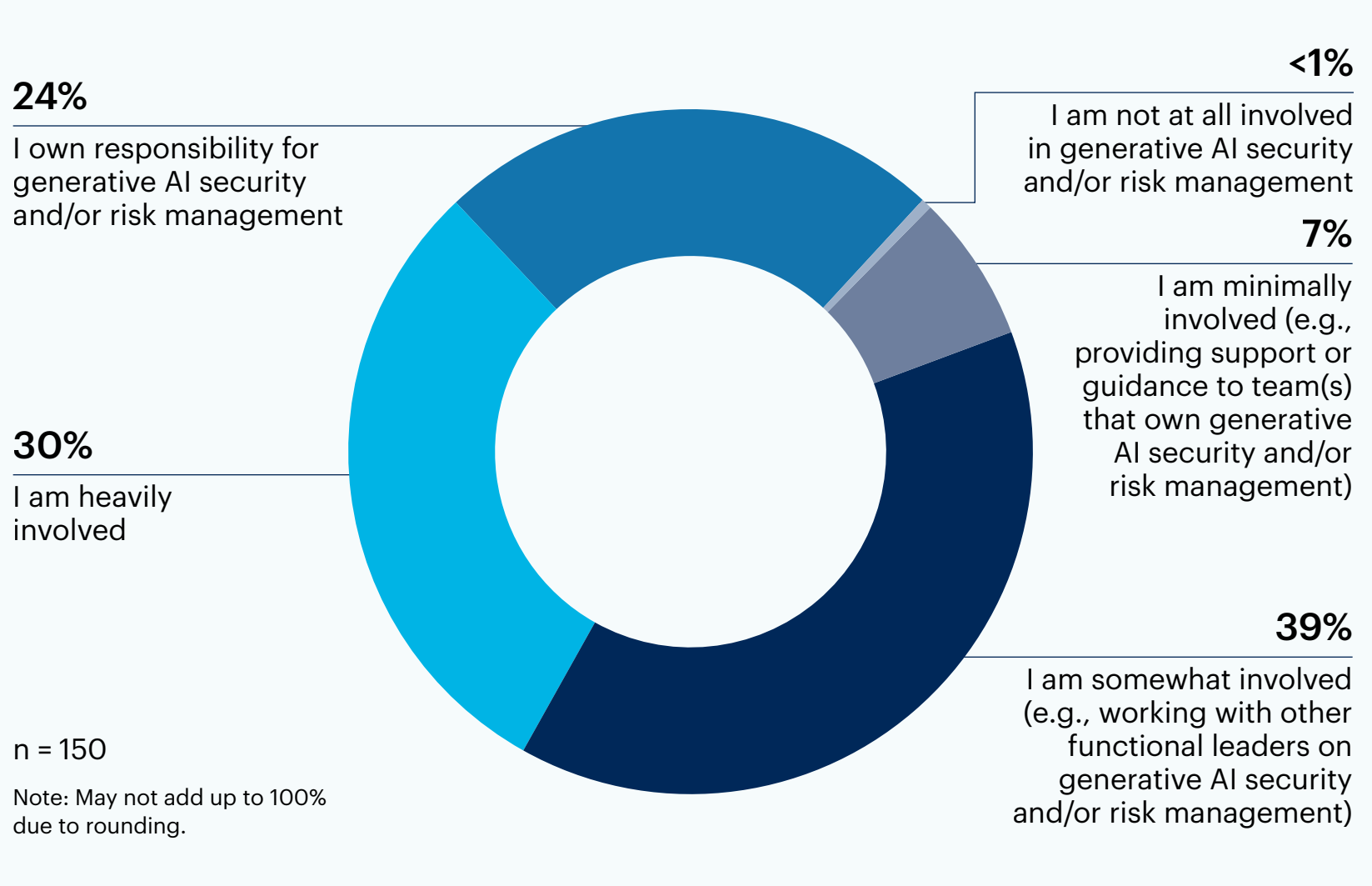
n = 150

Note: May not add up to 100% due to rounding.

*Respondents who answered No or Not sure were eliminated from the survey.

Nearly all (93%) IT/security leaders surveyed are at least somewhat involved in their organization's generative AI security/risk management efforts, but just 24% say they own this responsibility.

Are you involved in security and/or risk management efforts related to the use of generative AI tools or foundational models in your organization?

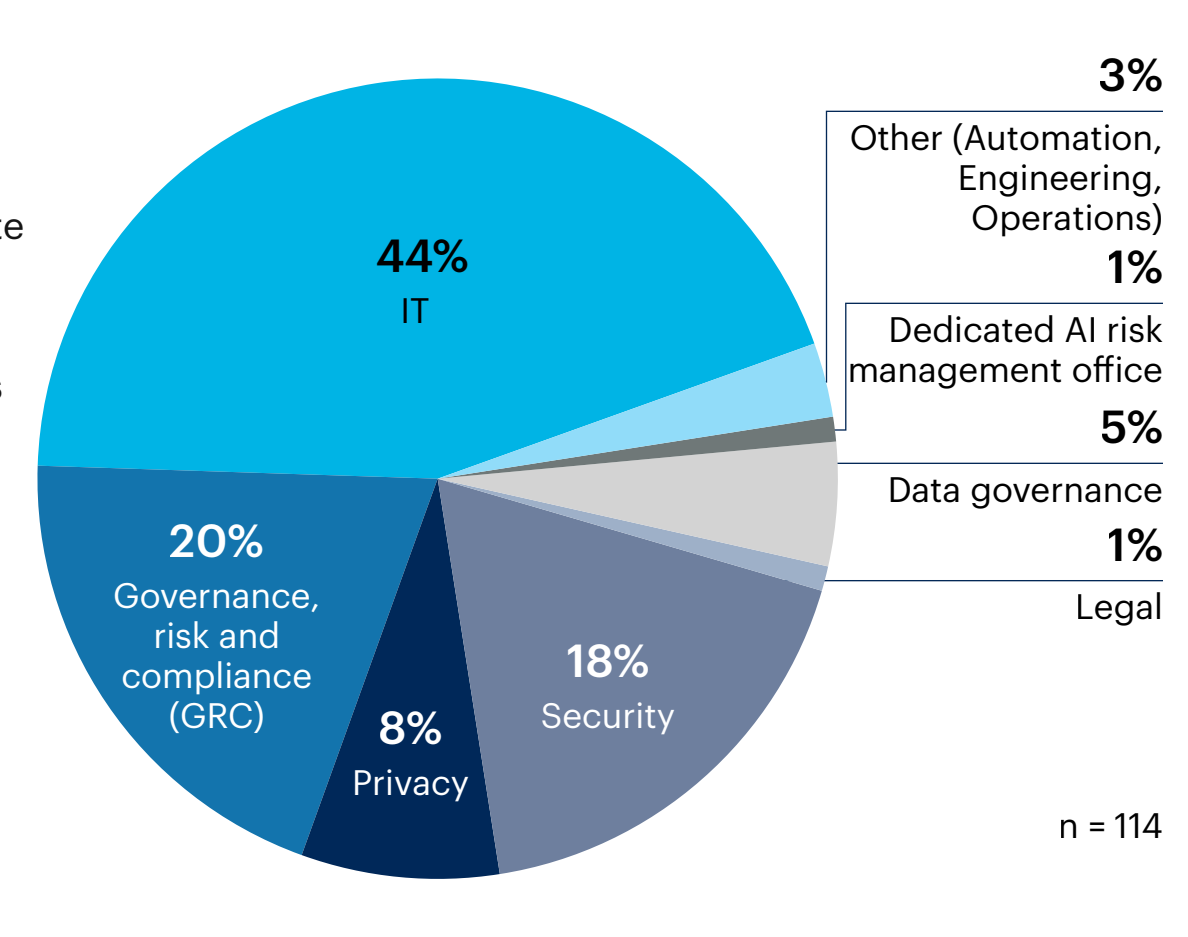


n = 150

Note: May not add up to 100% due to rounding.

Among those respondents that do not own the responsibility for generative AI security and/or risk management (n =114), most indicate that ultimate responsibility for generative AI security commonly rests with IT (44%), but 20% say it's owned by their organization's governance, risk, and compliance (GRC) function.

Which function or group in your organization is ultimately responsible for generative AI security?*



n = 114

Note: May not add up to 100% due to rounding.

*Question shown only to leaders who did not answer "I own responsibility for generative AI security and/or risk management" to the question "Are you involved in security and/or risk management efforts related to the use of generative AI tools or foundational models in your organization?"

> "AI is over hyped right now, we need to wait a bit to clear our minds."
>
> - Director, biotech industry, 1,000 - 5,000 employees

> "This is a new area and all our decisions are being questioned constantly."
>
> - C-suite, professional services industry, 1,000 - 5,000 employees

> "[W]e are still in the learning and discovery phase."
>
> - Director, transportation industry, 5,000 - 10,000 employees

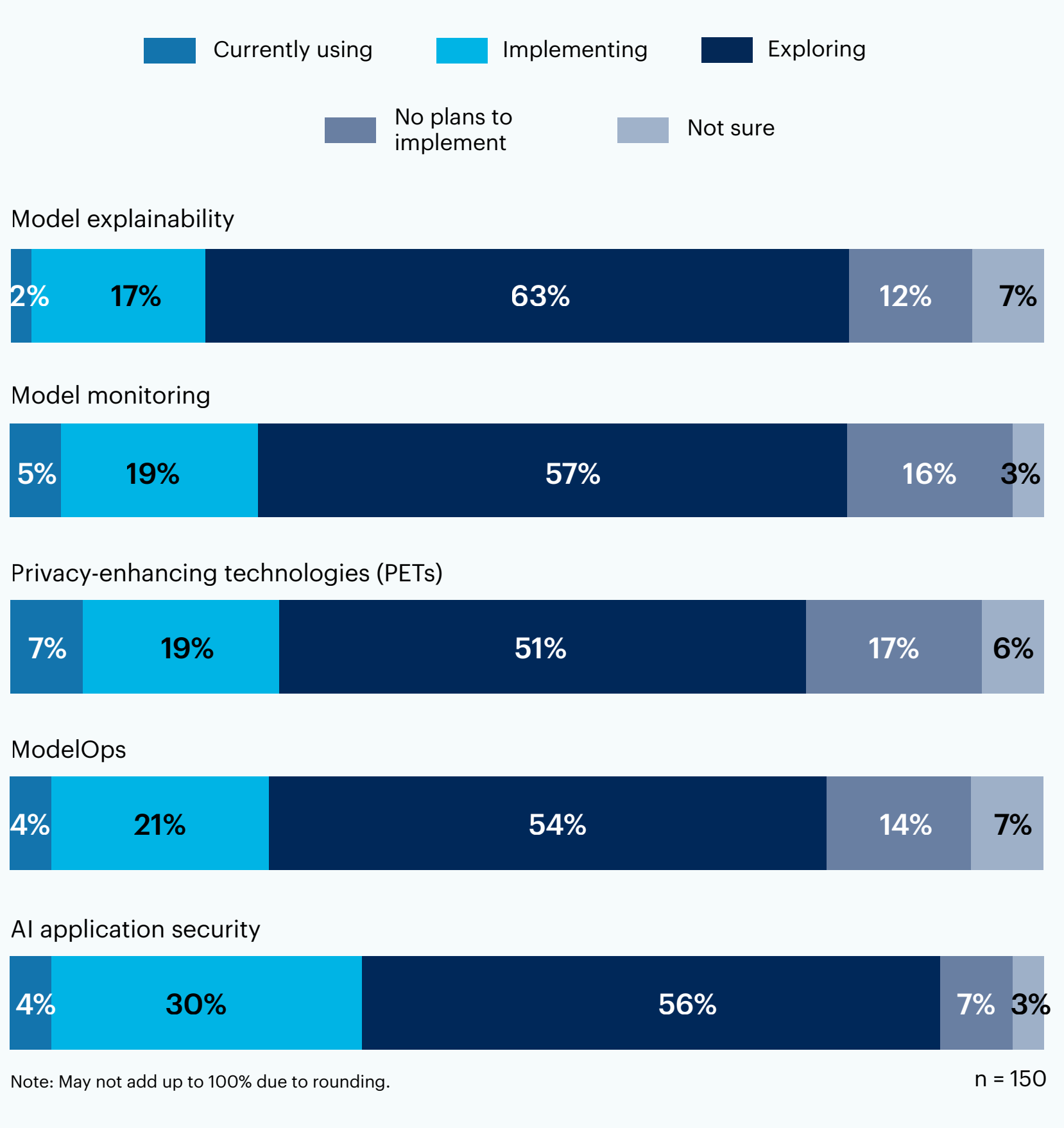
Question: Please share any final thoughts on your experience on generative AI risk mitigation and security.

The vast majority have or are looking to incorporate tools in their generative AI security and risk management strategy

34% of all respondents are either already using or implementing AI application security tools and over half (56%) are exploring such solutions.

Some respondents indicate that they are currently implementing or using privacy-enhancing technologies (PETs) (26%), ModelOps (25%) or model monitoring (24%). Only 19% are using or implementing tools for model explainability.

Are you using or planning to use tools for any of the following to address risks related to generative AI?



Note: May not add up to 100% due to rounding. n = 150

> "Leveraging our own technology for this one."
>
> - C-suite, software industry, 10,000+ employees

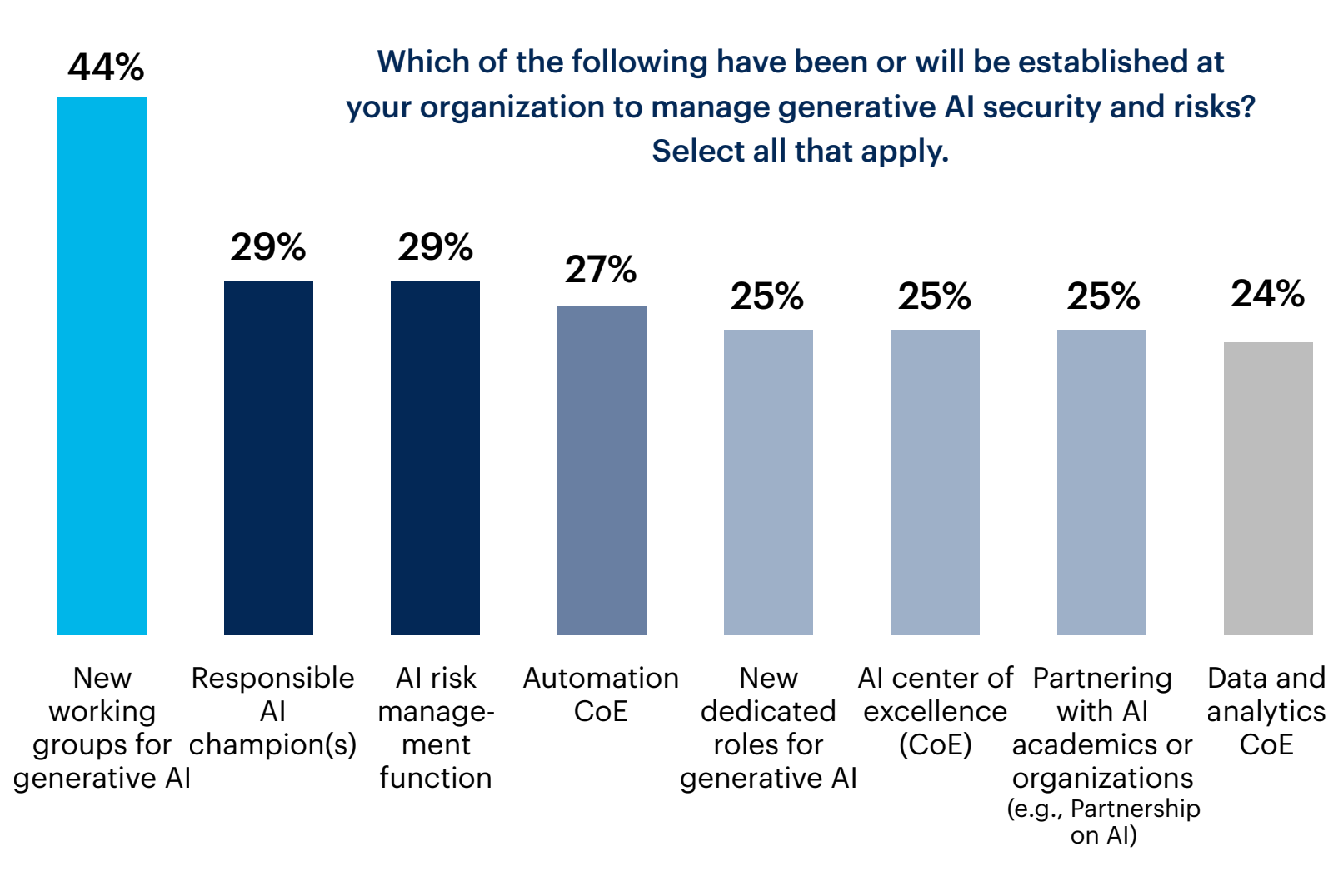
> "Early days for this technology, so we are proceeding with curiosity and trying not to get caught up in the hype cycle."
>
> - C-suite, consumer goods industry, 1,000 - 5,000 employees

Question: Please share any final thoughts on your experience on generative AI risk mitigation and security.

Respondents note responsible AI champions and data guidelines among security and risk management strategies for generative AI

44% of respondents say their organization has or will establish new working groups to manage generative AI security and risks.

Some report that their organization has or is looking to centers of excellence for automation (27%), AI (25%) or data and analytics (24%) to manage security and risks associated with this tech. One-quarter (25%) say their organization has or will add new dedicated roles for generative AI, and just as many cite partnerships between their org and AI academics or organizations (25%).

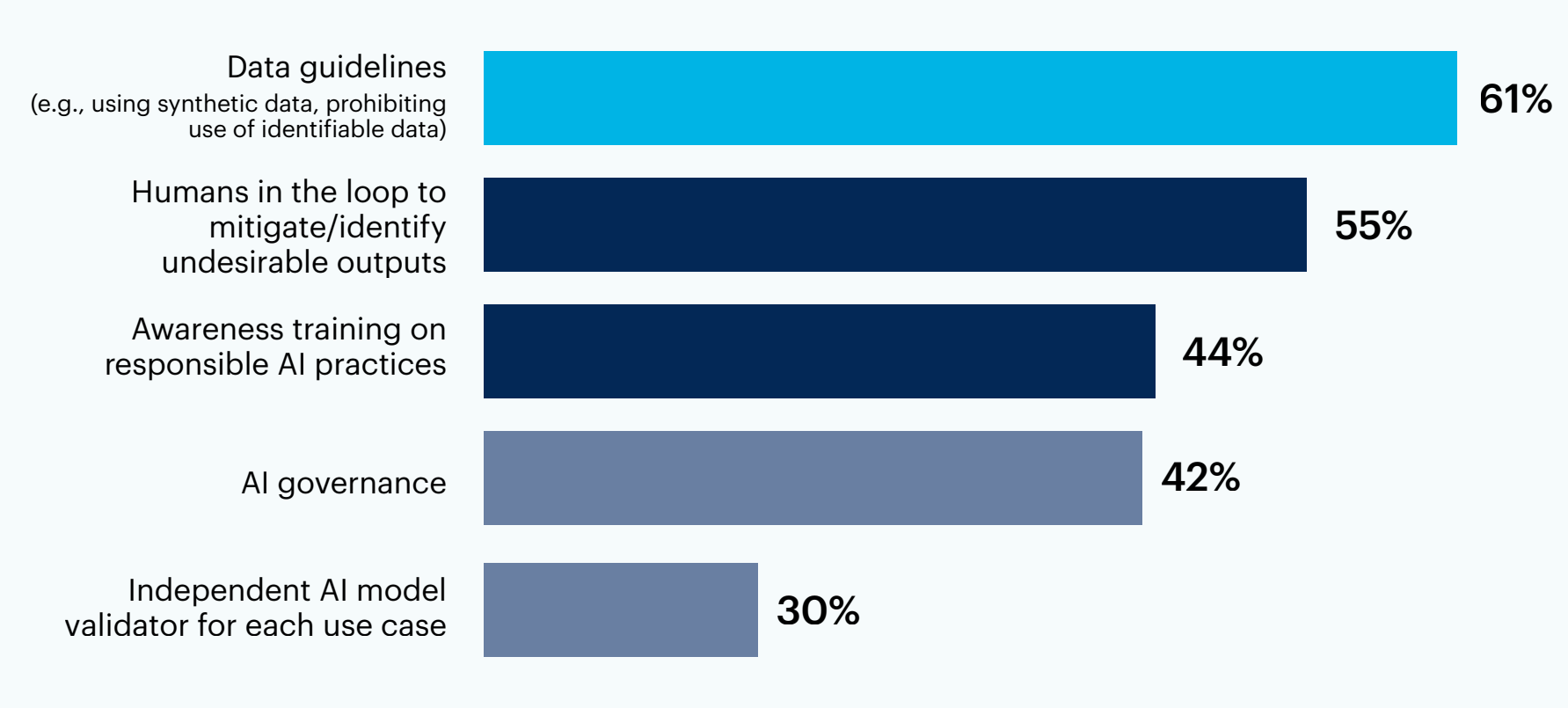


AI ethics board **14%** | Partnering with AI startups **12%** | Not sure **7%** | None of these **4%** | Other (Too early to say) **1%**

n = 150

Most respondents use or plan to use data guidelines (61%) and humans in the loop (55%) to mitigate risks associated with generative AI tools or foundational models.

What strategies are you using or planning to use to mitigate risks associated with the use of generative AI tools or foundational models? Select all that apply.



Vendor selection strategies (e.g., requiring explainable AI) **21%** | AI application security program **20%** | Explainable AI frameworks **19%** | Adversarial attack resistance **17%** | Not sure **5%** | Other **<1%** | None of these **0%**

n = 150

> "[W]e are still early in the implementation and are primarily focused on risk and [cybersecurity]. We are confident that it is vetted for our healthcare and clinician workflows without human intervention. Not worth the expense at this point for that."
>
> - C-suite, healthcare industry, 1,000 - 5,000 employees

> "It's not 100% fool-proof and still benefits from human intervention."
>
> - Director, healthcare industry, <1,000 employees

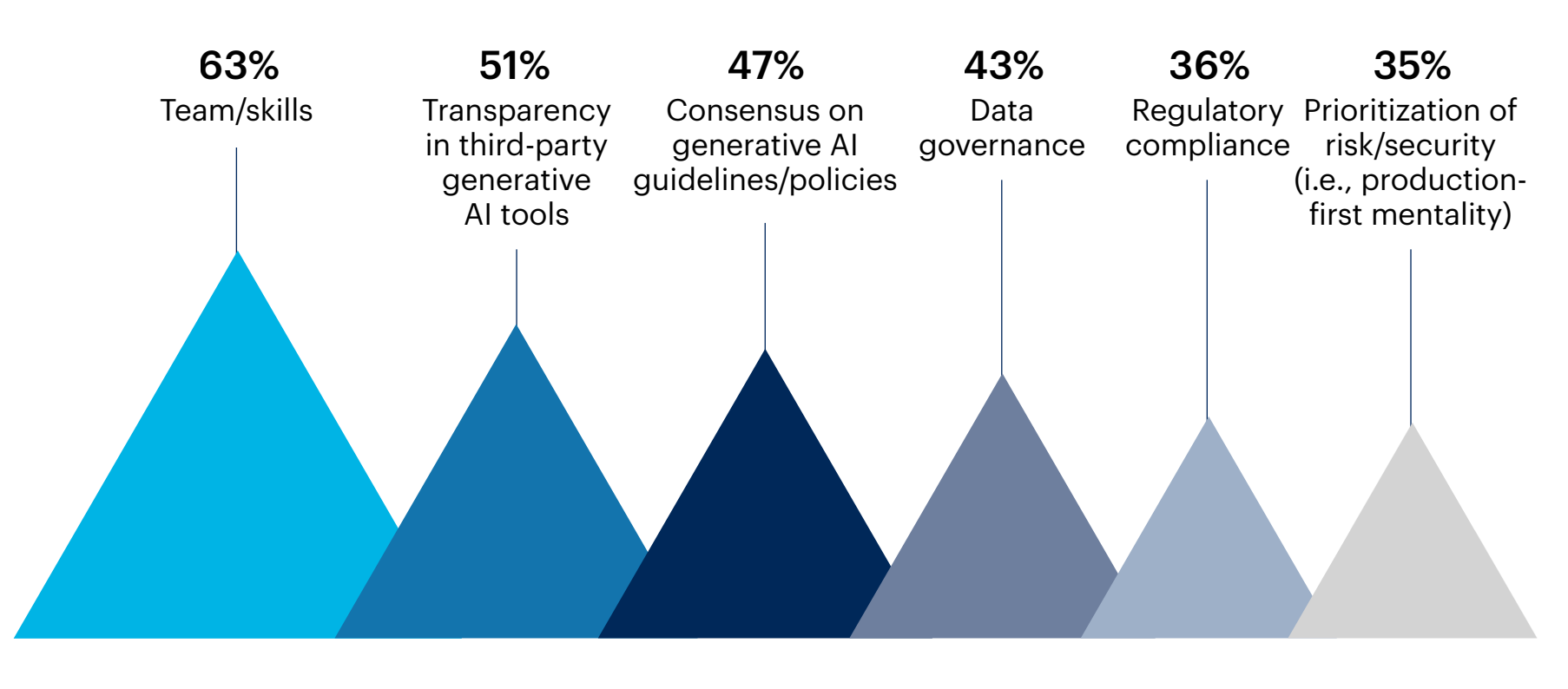
> "We are currently assessing compliance aspects [and] static analysis tool capabilities to continuously scan AI generated code, and also forming guidelines for aware and ethical use of generative AI tools by engineers."
>
> - C-suite, finance industry, <1,000 employees

Question: Please share any final thoughts on your experience on generative AI risk mitigation and security.

Undesirable outputs and insecure code are among the top-of-mind risks concerning most respondents in terms of generative AI at their organizations

When it comes to deficiencies in security and risk management for generative AI or foundational models, surveyed leaders noted gaps in team/skills (63%), transparency in third-party generative AI tools (51%), and consensus on related guidelines or policies (47%).

Are you experiencing gaps or deficiencies in any of these areas when it comes to security/risk management for generative AI tools or foundational models? Select all that apply.



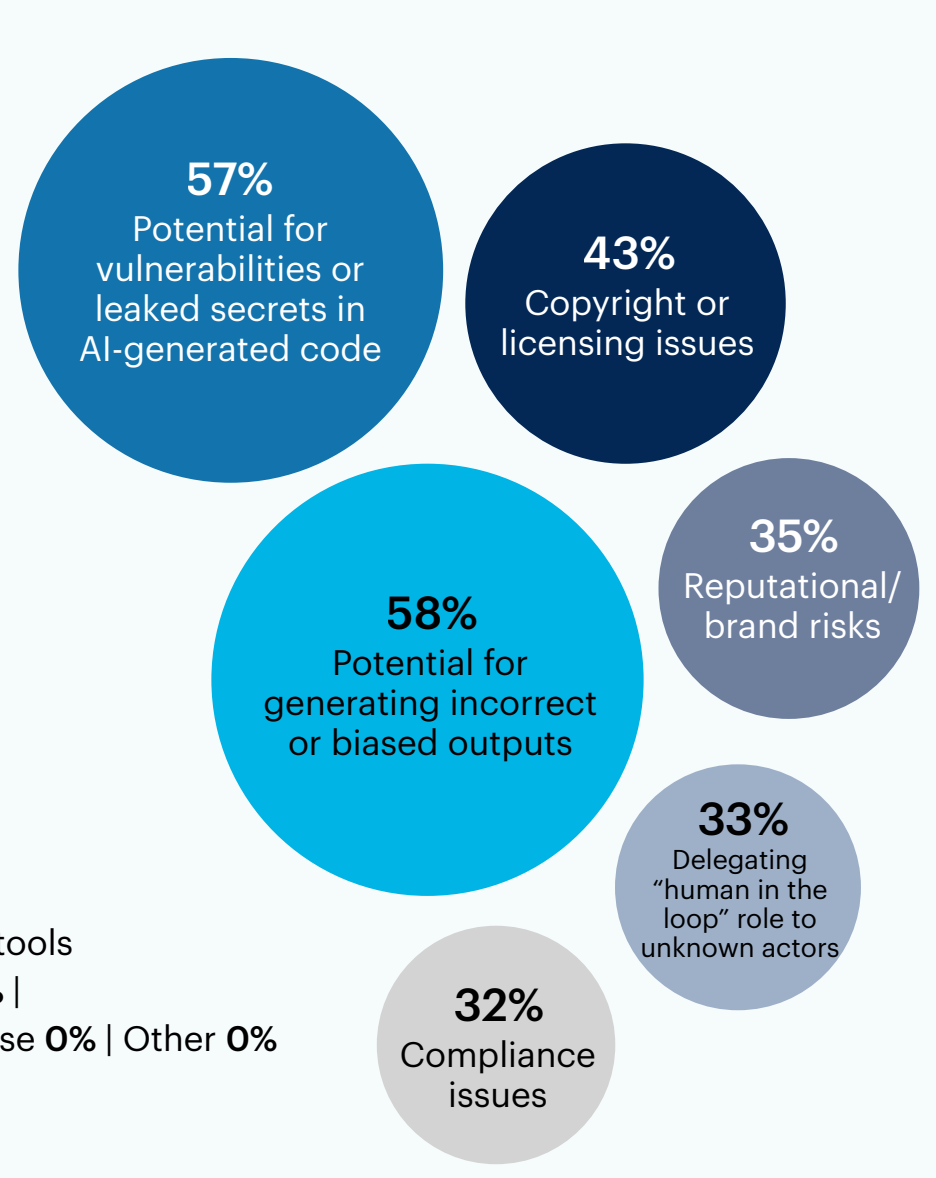
Industry best practices **29%** | Transparency in foundational models **21%** | Collaboration across stakeholder groups **17%** | Not sure **2%** | None of these **1%** | Other **0%**

n = 150

More than half of respondents say the risks they are most concerned about for their organization include incorrect or biased outputs (58%) and vulnerabilities or leaked secrets in AI-generated code (57%).

Many identified copyright or licensing issues (43%) among their risks of greatest concern for their organization.

What risk(s) are you most concerned about for your organization when it comes to generative AI tools or foundational models? Select up to three.



Increasing availability of ready-to-use generative AI tools (e.g., limited ability to restrict employee access) **21%** | Data re-identification **17%** | Not sure **1%** | None of these **0%** | Other **0%**

n = 150

> "Loss of internal IP is rising to the top of our list as the number 1 risk for ChatGPT use within our organization with the potential for developers to feed it source code to help improve quality."
>
> - VP, natural resource extraction industry, 10,000+ employees

> "There is still no transparency about data models are training on, so the risk associated with bias, and privacy is very difficult to understand and estimate."
>
> - C-suite, finance industry, <1,000 employees

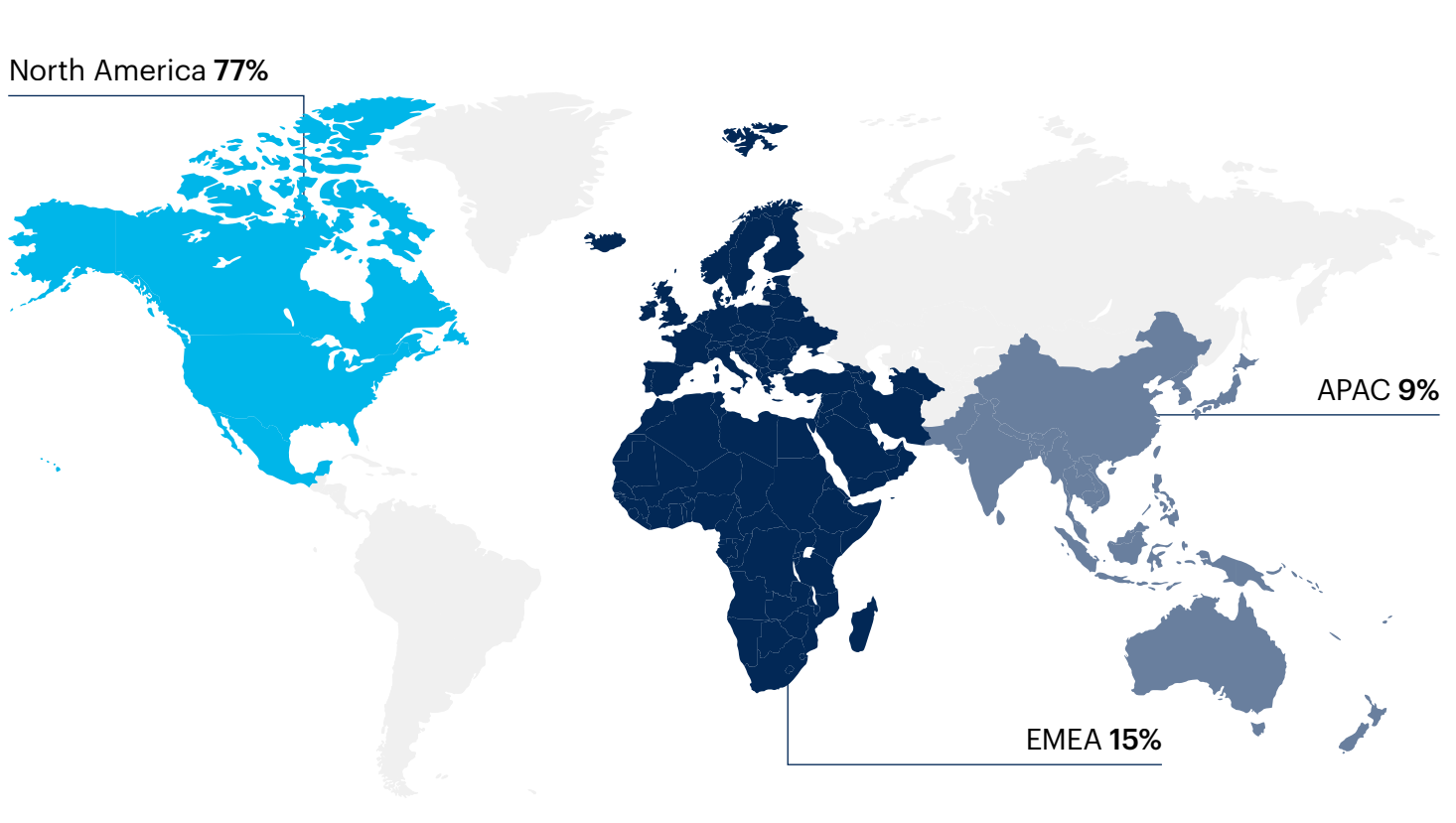
Question: Please share any final thoughts on your experience on generative AI risk mitigation and security.

Want more insights like this from leaders like yourself?

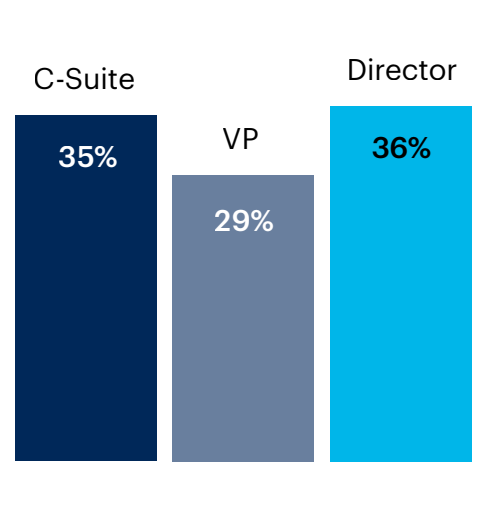
Click here to explore the revamped, retooled and reimagined Gartner Peer Community. You'll get access to synthesized insights and engaging discussions from a community of your peers.

Respondent Breakdown

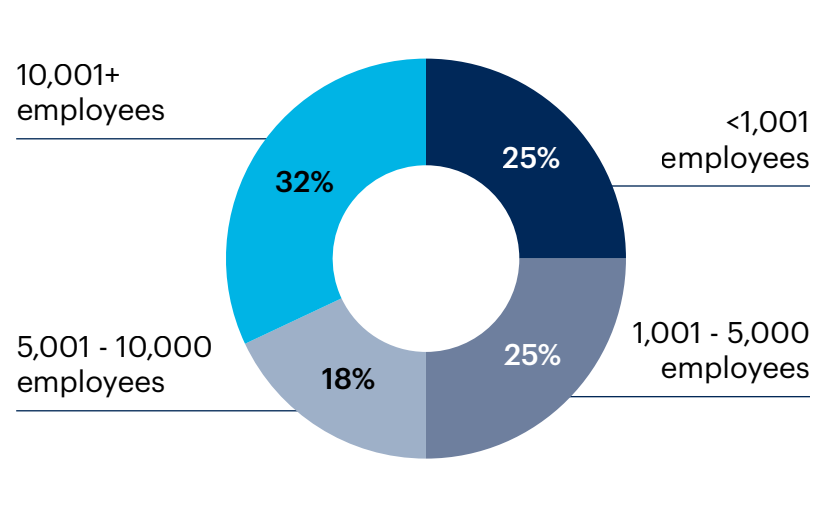
Region



Job Level



Company Size



Note: May not add up to 100% due to rounding.

Respondents: 150 IT and information security leaders at organizations where generative AI or foundational models are in use, in plans for use, or being explored

Gartner

Source: Gartner Peer Community, Generative AI Security and Risk Management Strategies survey