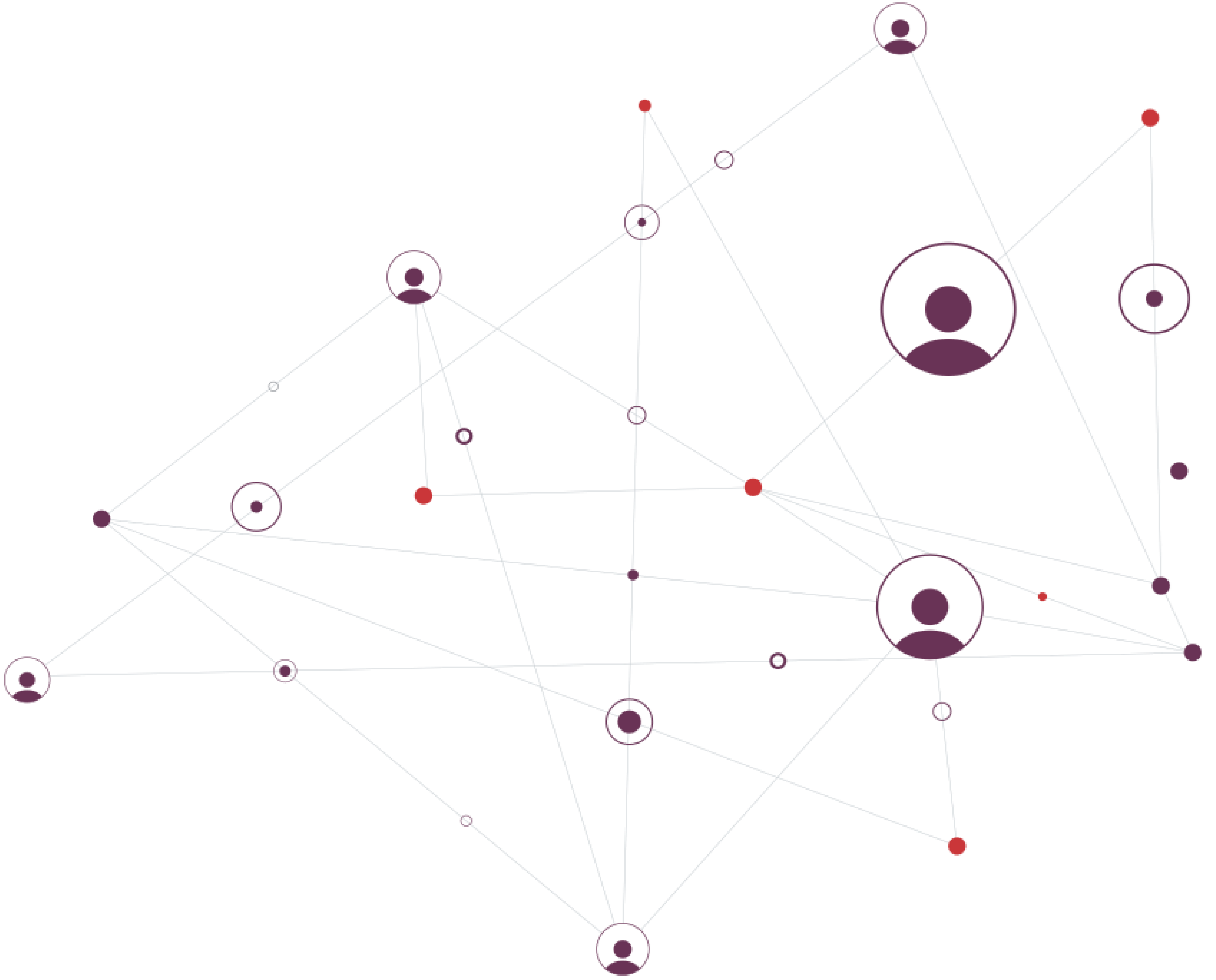
Market Connections™
Research you can act on.



US Next-Gen Government IT: AI and Observability Insights

February 2025

Presented to: SOLARWINDS

Methodology

PRIMARY OBJECTIVES:

SolarWinds partnered with Market Connections to conduct an online survey in December 2024, targeting 200 US IT decision-makers and influencers from Federal, State and Local, and Education sectors, along with 100 public sector counterparts in the UK. This report focuses on findings from the US audience, with UK results available in a separate report.

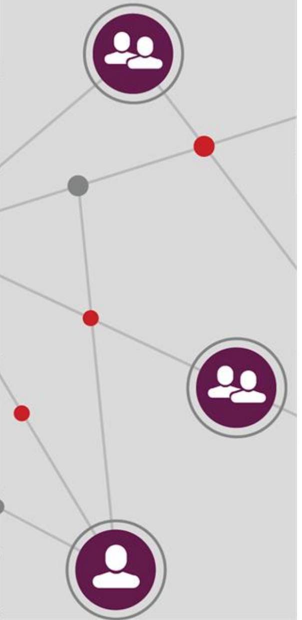
- Identify challenges faced by public sector IT professionals and sources of IT security threats
- Assess confidence levels and concerns related to managing the IT environment
- Explore barriers to achieving digital modernization
- Examine the current state of visibility and observability
- Evaluate the usage and implementation of artificial intelligence (AI)

Key Findings

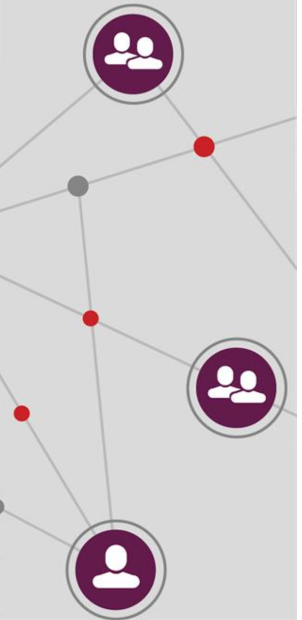
The public sector continues to navigate a rapidly evolving technology landscape. As organizations increasingly transition workloads to the cloud and adopt hybrid IT environments, the challenge of ensuring data security becomes ever more complex. For over a decade, SolarWinds has been tracking cybersecurity trends, challenges, and solutions in the public sector to provide valuable insights into this dynamic environment.

This year is no exception. We explored today’s most pressing security challenges, including vulnerabilities in monitoring systems and the critical need to safeguard sensitive information from cyber threats. We examined the visibility gap that emerges as agencies move from legacy on-premises systems to hybrid and cloud architectures. Additionally, we investigated the integration of AI and AIOps in observability solutions and how agencies are leveraging these tools to automate tasks, enhance issue identification and resolution, and improve overall IT operations.

The key findings on the following pages highlight the challenges facing public sector organizations and provide a comprehensive look at the current state of IT security and observability.



Key Findings



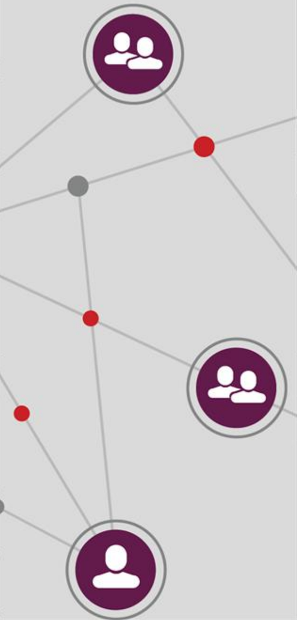
Over Half of Respondents Identify the General Hacking Community as the Leading Source of IT Security Threats

The general hacking community (59%) followed by careless or untrained insiders (58%) emerge as the greatest sources of security threats, emphasizing the need for stronger security awareness training, enhanced tools, and better access control mechanisms. While foreign governments remain a notable concern, with 51% of respondents identifying them as a top threat, this has declined from its position as the leading threat in 2023 (60%). This shift highlights the evolving threat landscape and the importance of addressing both internal and external vulnerabilities effectively.

Only 6% Have Fully Completed Their Digital Transformation Journey

Most report being in the early or middle stages of their digital transformation efforts. Challenges such as data privacy, security concerns, and the complexity of integrating new systems are key barriers. As agencies shift to hybrid IT, they face increasing pressure to manage data across diverse environments while ensuring seamless operations and compliance.

Key Findings



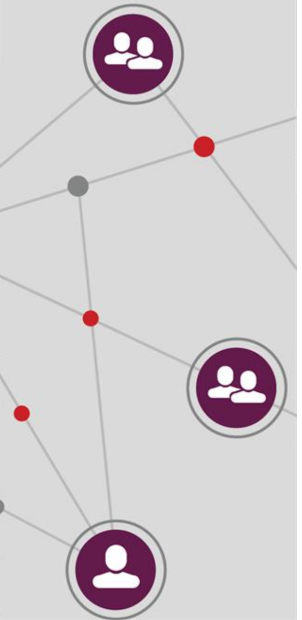
The Complexity of Managing Hybrid IT Environments Challenges Nearly Three-Quarters

Among respondents with hybrid IT environments, 73% report the complexity of managing it is challenging, with data protection and data privacy emerging as top security concerns. This complexity stems from the need to secure and integrate multiple infrastructures, including on-premises, private cloud, and public cloud environments. Additional challenges arise from data integration, monitoring, compliance, and ensuring seamless operations across these diverse systems. Respondents also recognize that the lack of visibility and standardization contributes to security gaps and operational inefficiencies.

Approximately Half See Observability as Extremely or Very Important for Accelerating Digital Transformation

Nearly half of respondents (48%) view observability as extremely or very important for accelerating digital transformation efforts, with enhanced security monitoring cited as the top benefit. Hybrid deployment models are the most preferred, followed by private cloud. However, security and privacy concerns are the top challenges to adopting observability tools, and effective implementation depends on addressing these issues while ensuring seamless integration across IT environments.

Key Findings



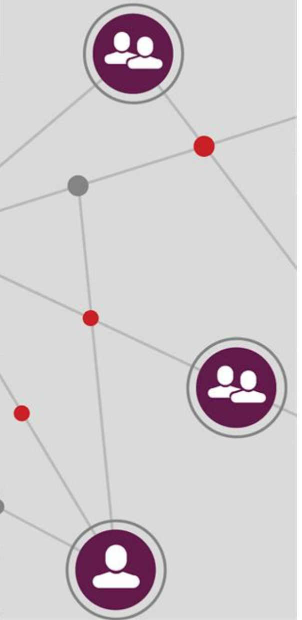
More Than One-Third Report Using AI to Automate IT Operations and Observability

More than a third of respondents (35%) currently leverage artificial intelligence (AI) to automate tasks related to IT operations and observability, with many more planning to adopt it soon. Predictive analytics and issue detection are seen as the most valuable aspects of AI, enabling proactive threat mitigation and optimization of IT performance. However, approximately four in ten are extremely or very concerned about potential risks associated with adopting AI, including data privacy and compliance, making full-scale implementation a cautious process.

Key Findings

As you read through the report and reflect on these key findings, you will note that they only scratch the surface of the complex challenges the public sector faces every day. At the same time, the findings highlight how agencies are harnessing the transformative potential of observability and AI to gain visibility into and effectively manage hybrid IT environments.

By deepening their understanding of how observability and AI can address their unique challenges, particularly in maintaining secure and efficient operations, the public sector will be well-positioned to harness the full power of these transformative tools.



VERBATIM COMMENTS

Challenges and Successes—Representative Comments

> Adopting a zero-trust architecture, we have significantly reduced the attack surface and improved our overall security posture.
>
> FEDERAL CIVILIAN

> Limited cybersecurity training on the part of students, teachers and administrators has made schools more susceptible to attacks.
>
> EDUCATION: HIGHER EDUCATION

> Technology is growing at such a rapid rate, and AI is becoming more prevalent. It has been beneficial in some regards, but it also comes with its own challenges. It's a matter of figuring out the right balance and how to best implement the proper strategies.
>
> DEFENSE/MILITARY

> It is becoming even more challenging to stay up-to-date with the rapid development of new technology.
>
> COUNTY GOVERNMENT

> Staying abreast of the rapid advancements in new technologies adds an additional level of complexity.
>
> STATE GOVERNMENT

> Trying to coordinate security policies across multiple federal agencies often leads to gaps.
>
> FEDERAL CIVILIAN

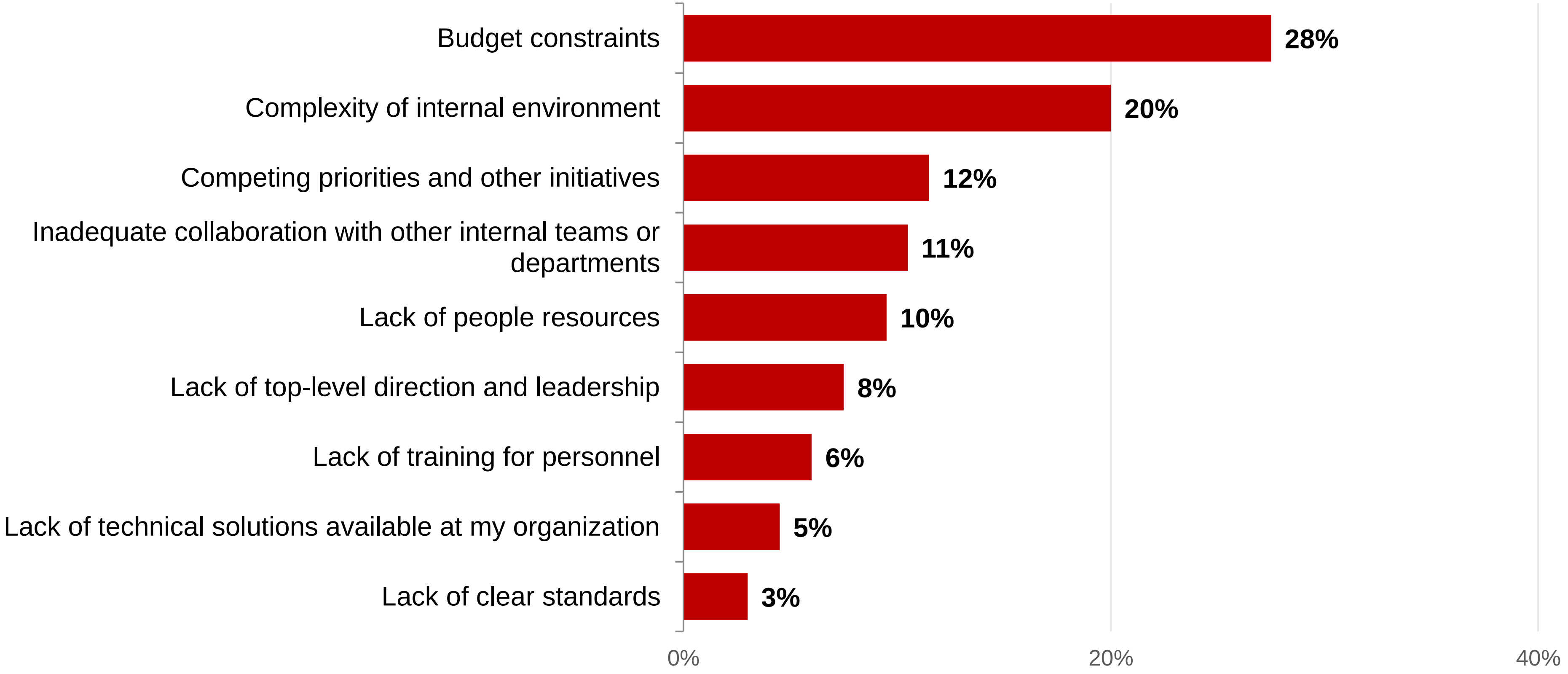
> Complexity and large amount of data is a great concern.
>
> DEFENSE/MILITARY

> We may be unable to implement comprehensive security measures across all of our systems due to limited budget and resources.
>
> STATE GOVERNMENT

Q *Please feel free to share any other comments or concerns regarding your organization’s unique security challenges and/or success stories.*

IT Security Obstacles

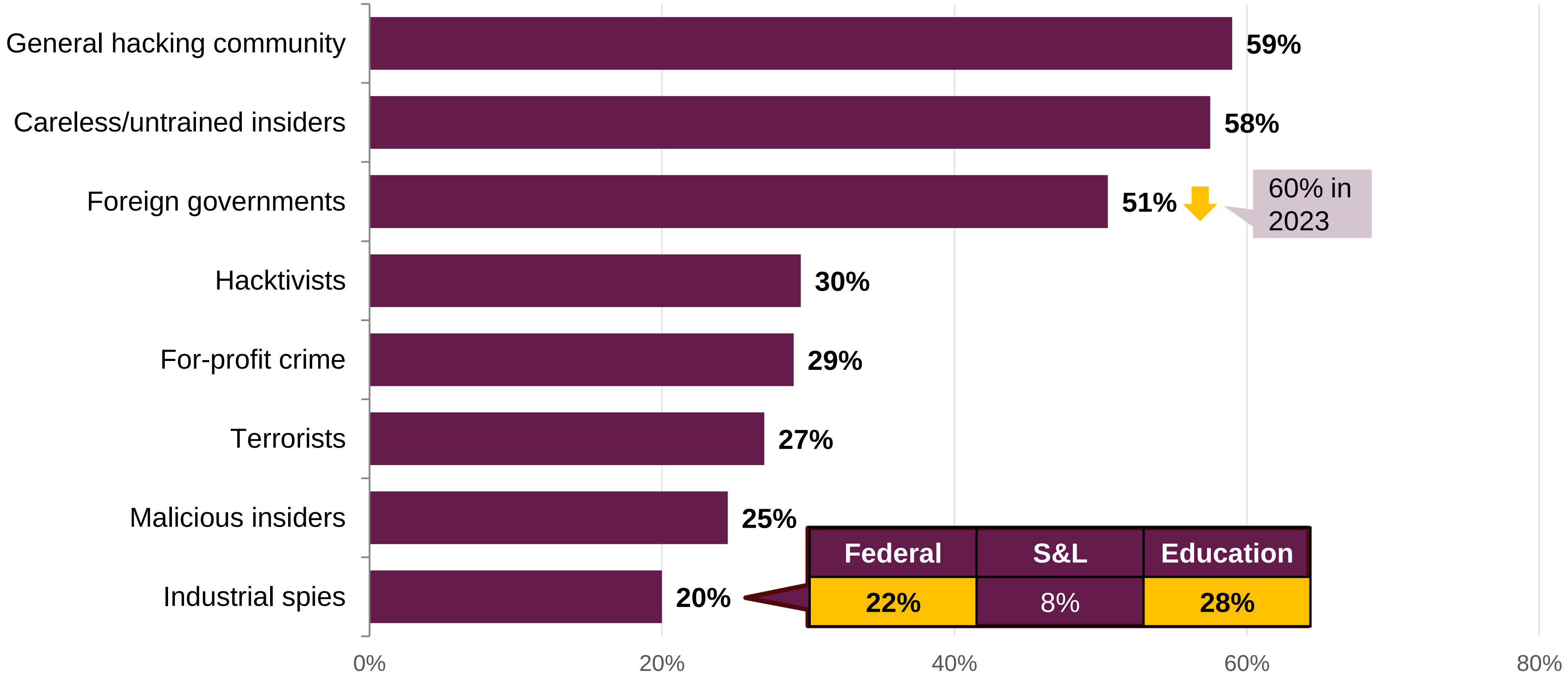
Budget constraints top this year's list of significant obstacles to maintaining or improving IT security. Closely following is the complexity of the internal environment.



Q *What is the most significant high-level obstacle to maintaining or improving IT security at your organization?*

Sources of Security Threats

The greatest sources of IT security threats are the general hacking community and careless or untrained insiders. Notably, the threat from foreign governments has significantly declined from its position as the top source in 2023.



60% in 2023

Industrial spies:

Federal	S&L	Education
22%	8%	28%

🟨 = significant differences between segments

Note: Multiple responses allowed

⬆⬇ = significant differences between 2023 and 2024

Q *What are the greatest sources of IT security threats to your organization? (select all that apply)*

Sources of Security Threats—Federal Trend

The top three sources of security threats have remained consistent for the federal audience since 2014, with careless or untrained insiders and the general hacking community reaching their highest levels over the years.

Federal	2014	2015	2016	2017	2018	2019	2021	2023	2024
Careless/untrained insiders	42%	53%	48%	54%	56%	52%	52%	58%	61%
General hacking community	47%	46%	46%	38%	48%	40%	56%	53%	60%
Foreign governments	34%	38%	48%	48%	52%	48%	59%	63%	52%
Terrorists	21%	18%	24%	20%	25%	22%	23%	27%	31%
Hacktivists	26%	30%	38%	34%	31%	26%	42%	38%	30%
For-profit crime	11%	14%	18%	17%	15%	20%	27%	22%	27%
Malicious insiders	17%	23%	22%	29%	36%	29%	30%	30%	25%
Industrial spies	6%	10%	16%	12%	19%	16%	23%	22%	22%

Note: Multiple responses allowed ■ = top three sources

Q *What are the greatest sources of IT security threats to your organization? (select all that apply)*

Sources of Security Threats—SLED Trend

The primary sources of security threats for the SLED audience have remained relatively consistent since 2019. However, in 2024, the education audience sees a shift, with the general hacking community surpassing careless or untrained insiders as the leading source of threats.

State and Local	2019	2021	2023	2024
Careless/untrained insiders	52%	51%	58%	52%
General hacking community	40%	63%	47%	50%
Foreign governments	48%	46%	56%	46%
Hacktivists	26%	43%	35%	32%
For-profit crime	20%	29%	18%	32%
Terrorists	22%	18%	23%	24%
Malicious insiders	29%	36%	28%	22%
Industrial spies	16%	21%	10%	8%

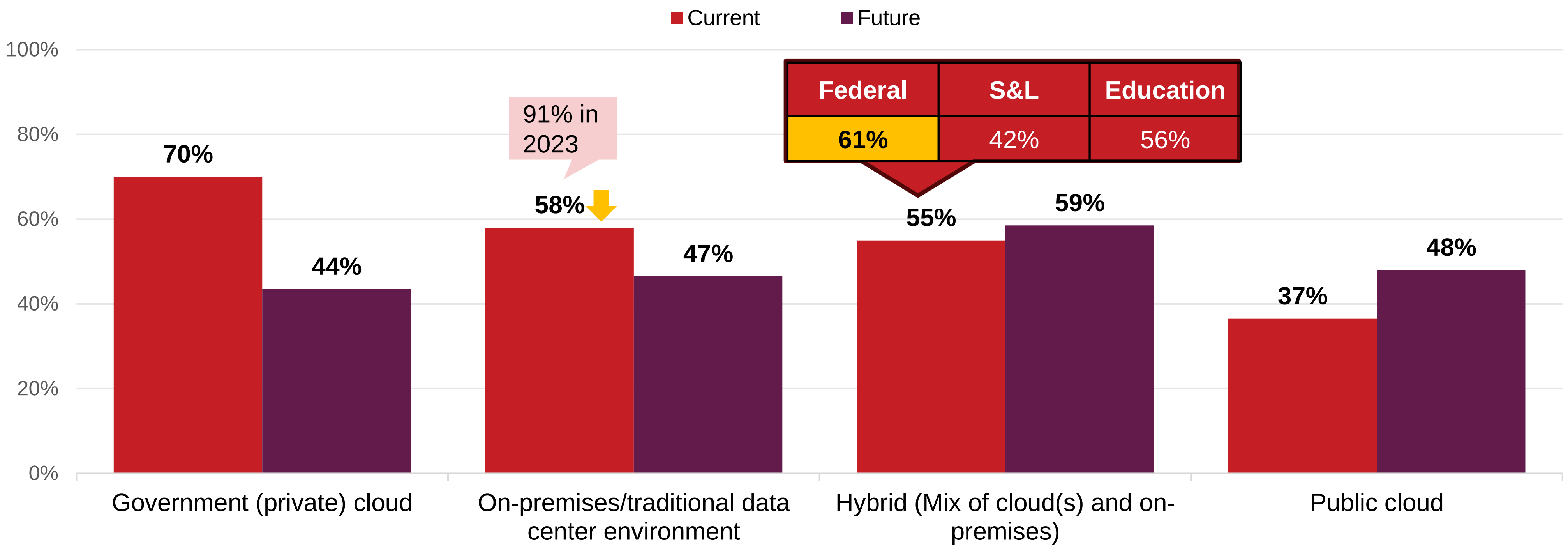
Education	2019	2021	2023	2024
General hacking community	40%	49%	55%	66%
Careless/untrained insiders	52%	53%	58%	56%
Foreign governments	48%	25%	56%	52%
For-profit crime	20%	25%	22%	30%
Industrial spies	16%	14%	13%	28% ↑
Hacktivists	26%	32%	38%	26%
Malicious insiders	29%	33%	25%	26%
Terrorists	22%	11%	22%	22%

Note: Multiple responses allowed ↑↓ = significant differences between 2023 and 2024 ■ = top three sources

Q *What are the greatest sources of IT security threats to your organization? (select all that apply)*

Current and Future IT Environment

In 2024, government (private) cloud has taken the lead as the most prevalent environment, driven by a decline in on-premises or traditional data center usage, which was the most common in 2023. Consistent with last year, respondents continue to anticipate that hybrid environments will be the most common in the future.



91% in 2023

Federal	S&L	Education
61%	42%	56%

🟨 = significant differences between segments

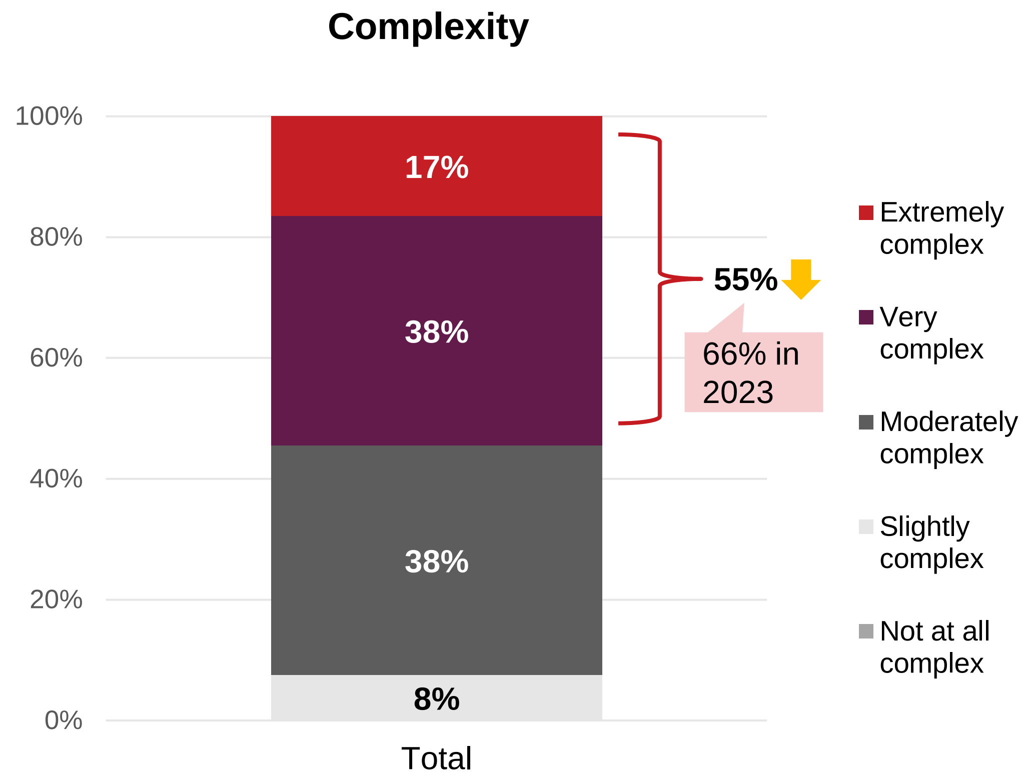
Note: Multiple responses allowed

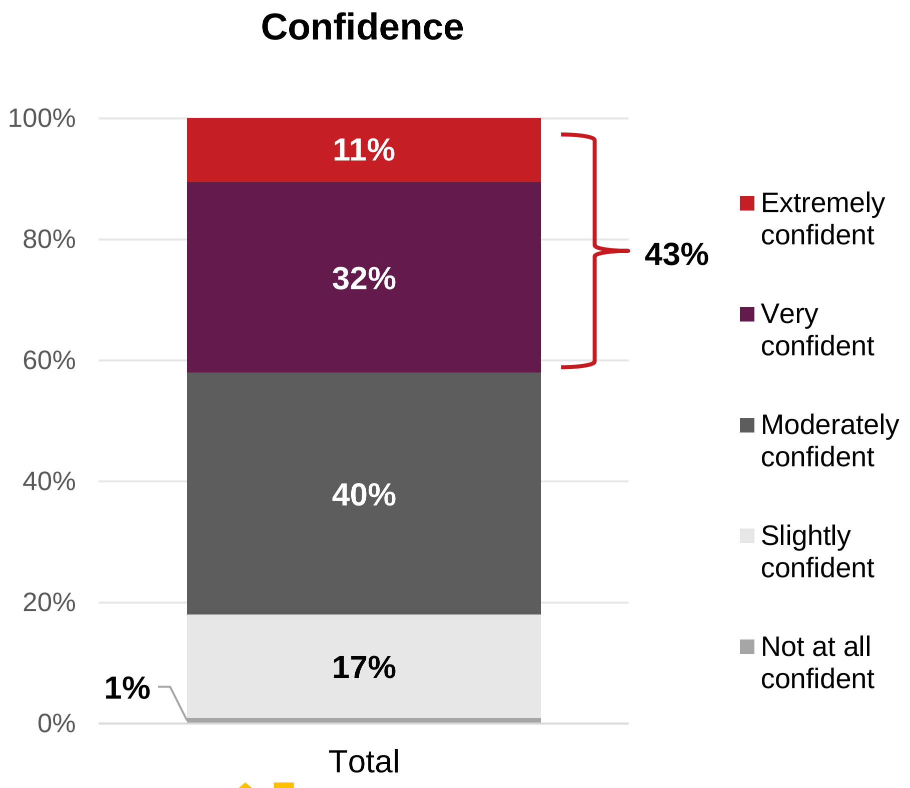
⬆⬇ = significant differences between 2023 and 2024

Q *Which of the following comprise your organization's IT environment? And which do you anticipate will comprise your organization's environment three years from now? (select all that apply)*

IT Environment Management Complexity and Confidence

Over half of respondents report their IT environment is extremely or very complex to manage, though this has decreased compared to last year. Additionally, less than half feel extremely or very confident in their ability to manage it effectively.





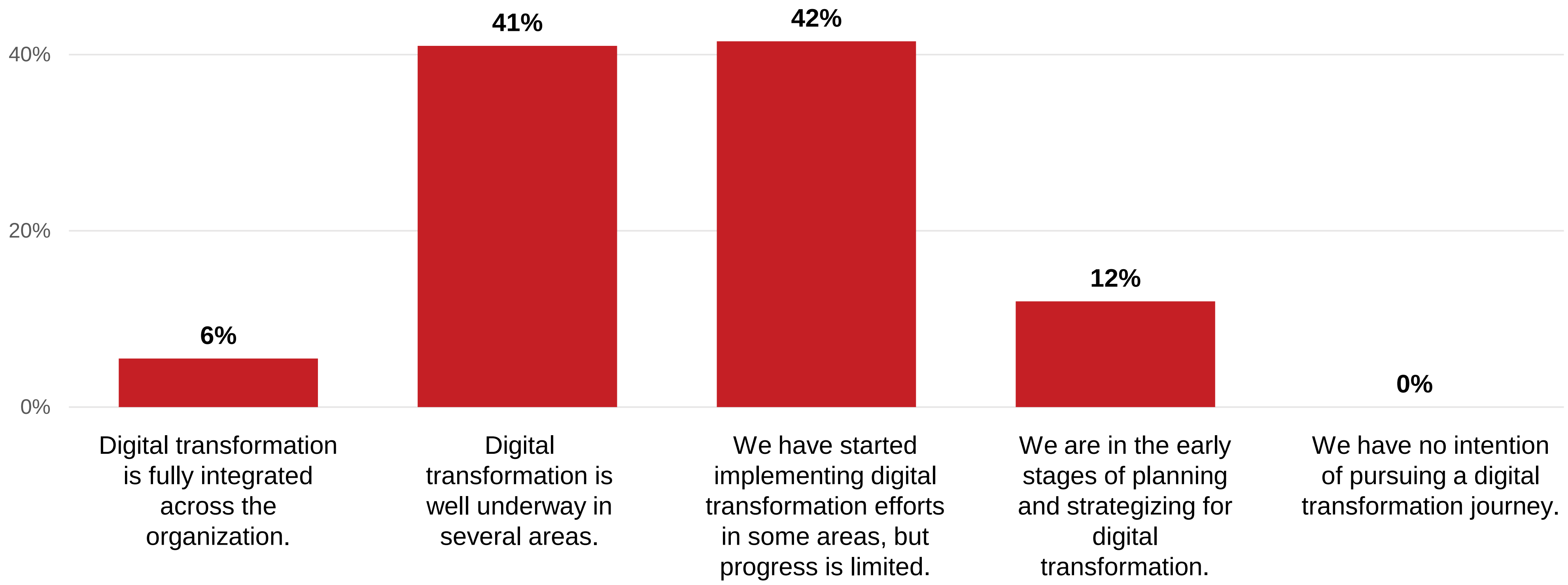
🟨 = significant differences between segments

⬆⬇ = significant differences between 2023 and 2024

Q *How complex is your organization’s IT environment to manage? How confident are you in your organization’s ability to manage its IT environment?*

Status of Digital Transformation Journey

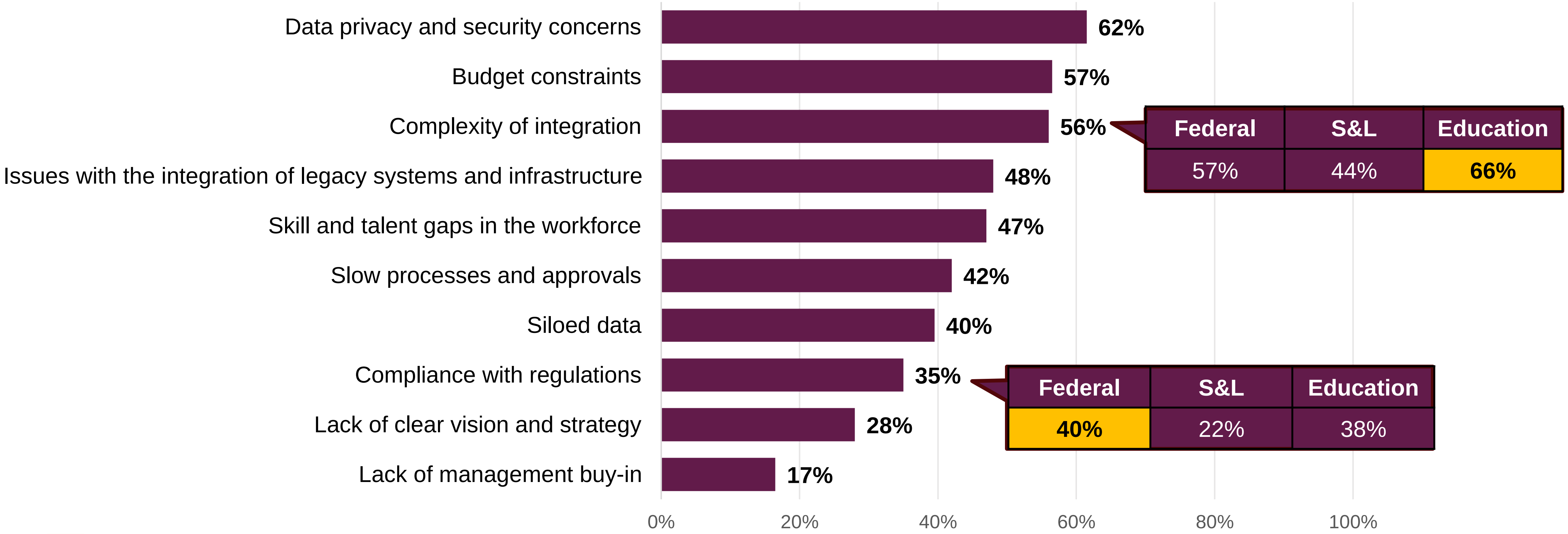
Only a small portion report that their organization has fully completed its digital transformation. Most indicate they are somewhere along the journey, with efforts either well underway or in the early stages of implementation.



Q *How far along is your organization in its digital transformation journey? Digital transformation means replacing non-digital or manual processes—many of which are key business drivers—with digital, software-based processes.*

Challenges in Digital Transformation

Data privacy and security concerns, budget constraints, and the complexity of integration are the top challenges in respondents' digital transformation journey. Notably, education-sector respondents are more likely to cite the complexity of integration as a challenge.



Complexity of integration:

Federal	S&L	Education
57%	44%	66%

Compliance with regulations:

Federal	S&L	Education
40%	22%	38%

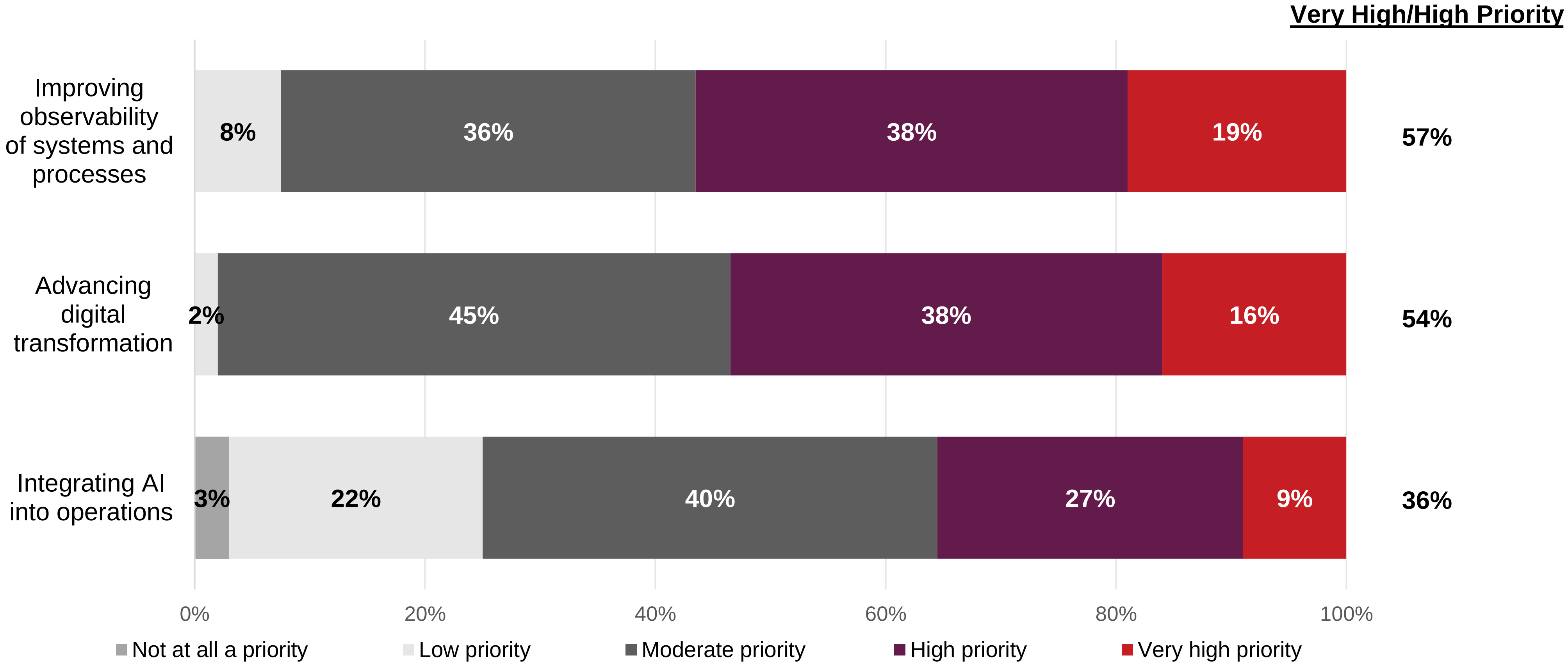
🟨 = significant differences between segments

Note: Multiple responses allowed

What challenges, if any, is your organization facing in its digital transformation journey? (select all that apply)

Future Priorities

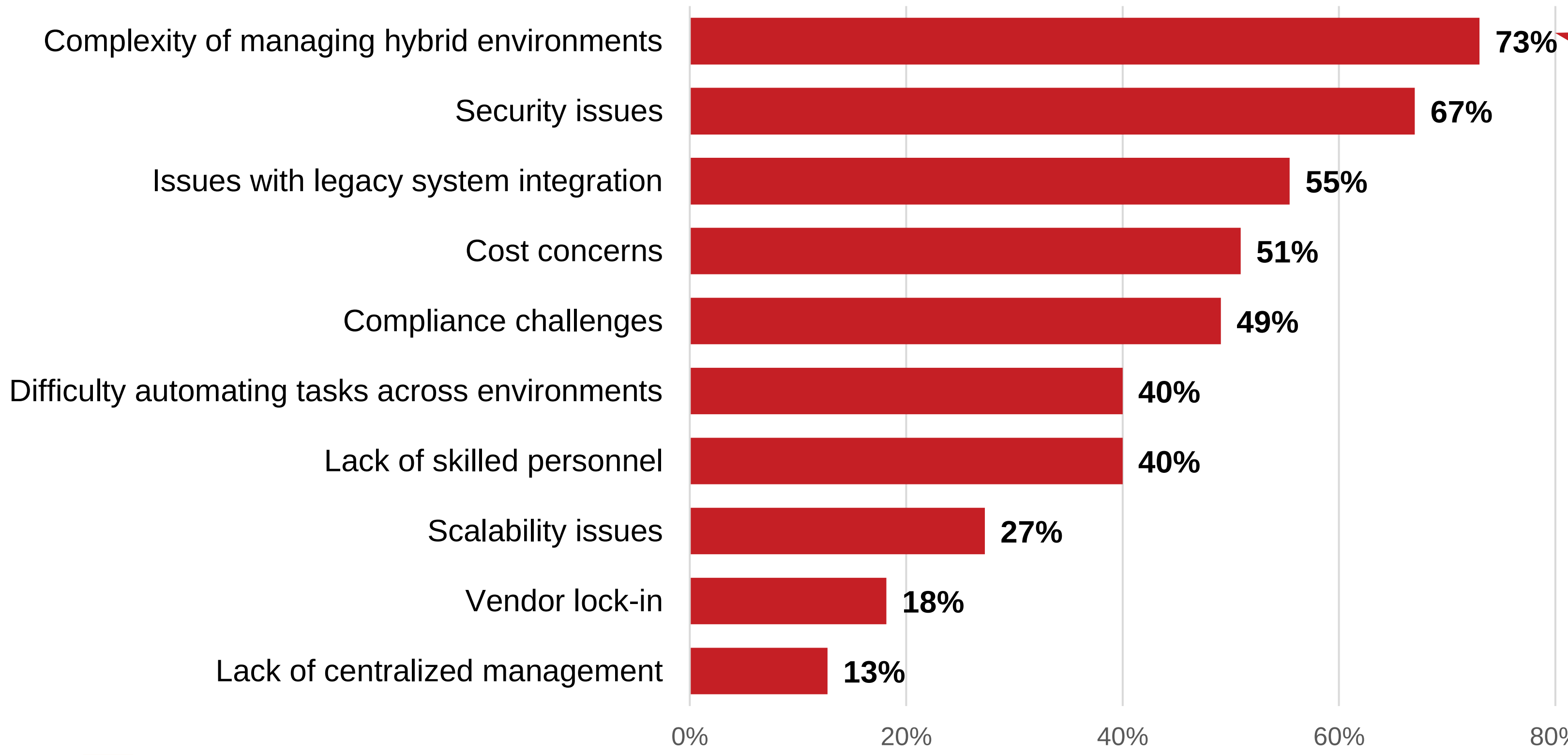
Improving the observability of systems and processes and advancing digital transformation are high or very high priorities for over half of the respondents. In contrast, integrating AI into operations is regarded as a lower priority.



How much of a priority are each of the following for your organization over the next 12 months?

Challenges in Hybrid IT Infrastructure

The complexity of managing hybrid environments is the top challenge, especially for federal respondents. Security issues, issues with legacy system integration, and cost concerns are also challenges for the majority.



Federal	S&L	Education
82%	62%	61%

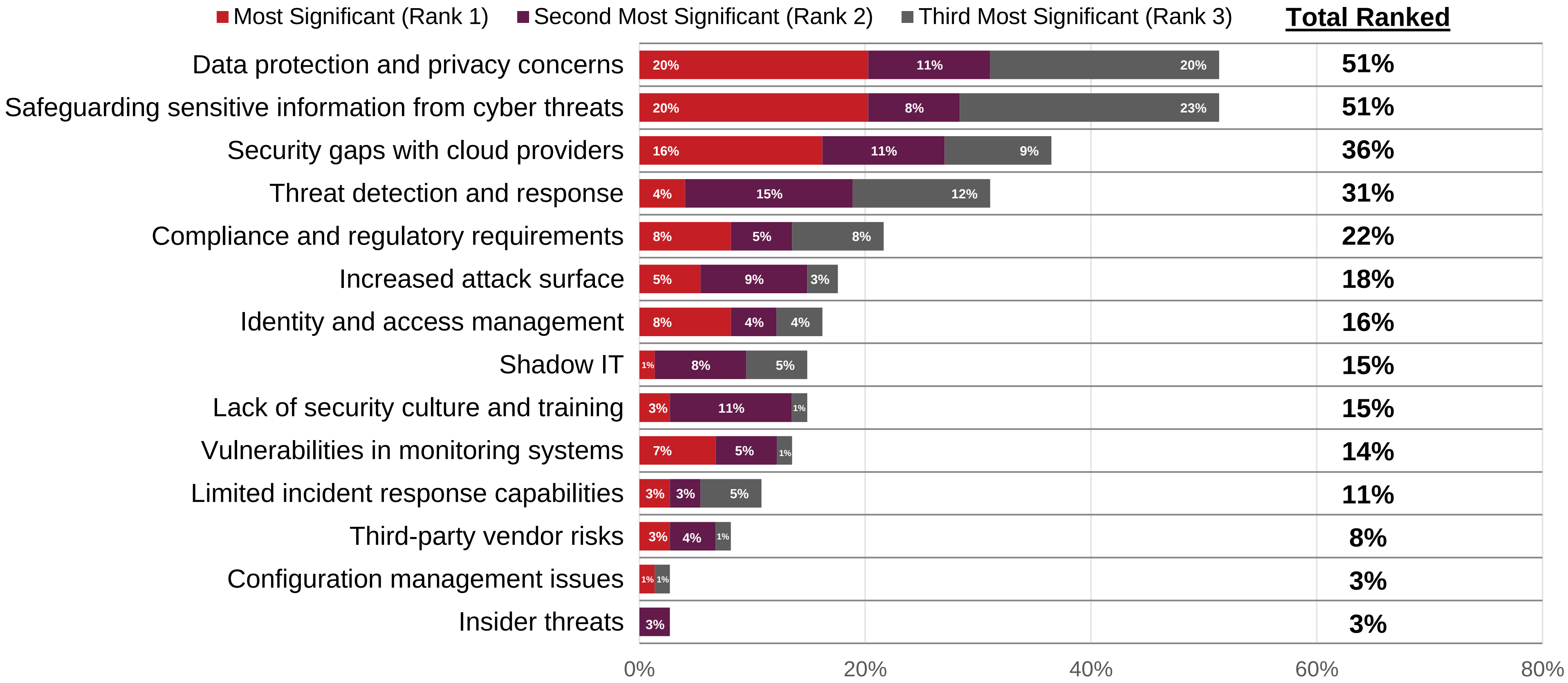
🟨 = significant differences between segments

Note: Multiple responses allowed

[IF HYBRID SELECTED FOR CURRENT ENVIRONMENT] Which of the following challenges, if any, does your organization face in managing its hybrid IT infrastructure? (select all that apply)

Top Security Challenges

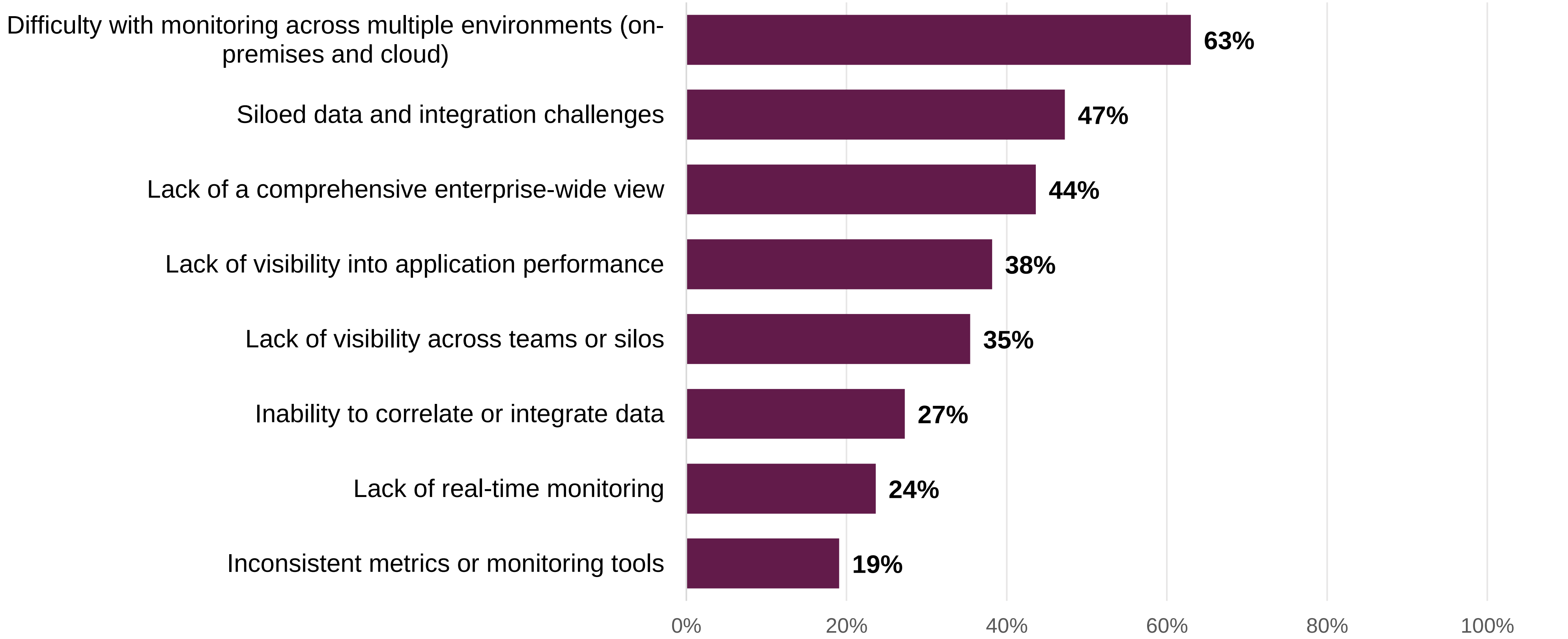
When considering both overall rankings and being ranked as the top priority, data protection and privacy concerns, along with safeguarding sensitive information from cyber threats, emerge as the leading security challenges in a hybrid IT infrastructure.



Q *[IF SECURITY ISSUES SELECTED IN PREVIOUS QUESTION] What are the most significant security challenges your organization faces in a hybrid IT infrastructure? Please rank up to 3, with #1 being the most significant.*

Challenges in Hybrid Visibility

Most respondents face challenges with monitoring across multiple environments, hindering their ability to gain visibility into their organization's hybrid IT infrastructure.

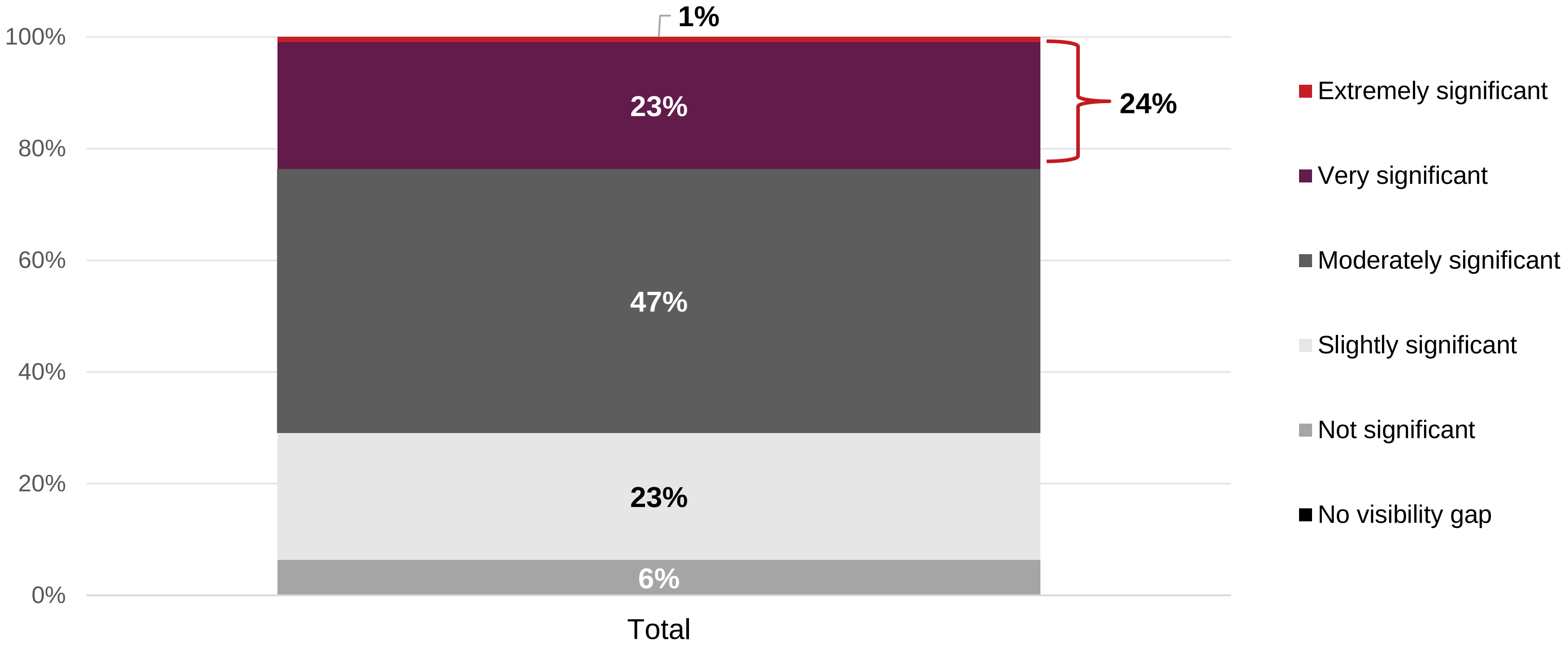


Note: Multiple responses allowed

Q *Which of the following challenges, if any, does your organization face in gaining visibility into its hybrid IT infrastructure? (select all that apply)*

Visibility Gap in Hybrid Environment

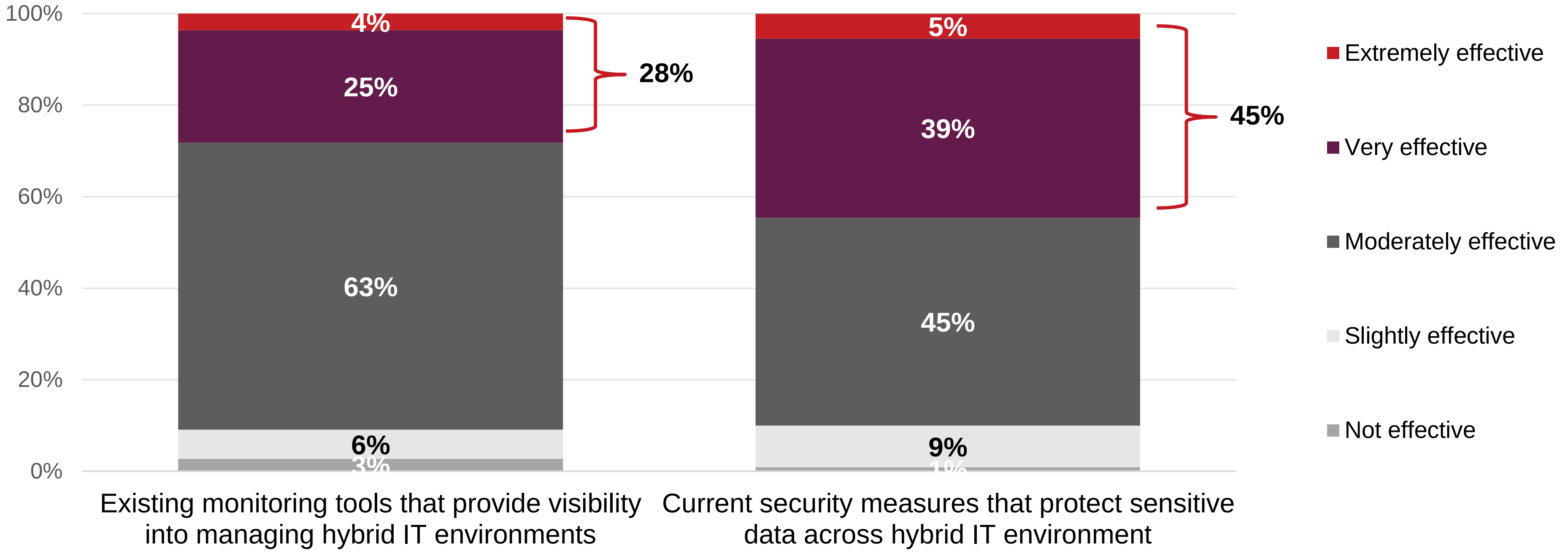
The visibility gap is a recognized challenge for most hybrid organizations, with a quarter indicating it is extremely or very significant and nearly half considering it moderately significant.



How significant is the visibility gap (i.e., the lack of full visibility or monitoring capabilities) in your organization's hybrid IT environment?

Current Hybrid Management

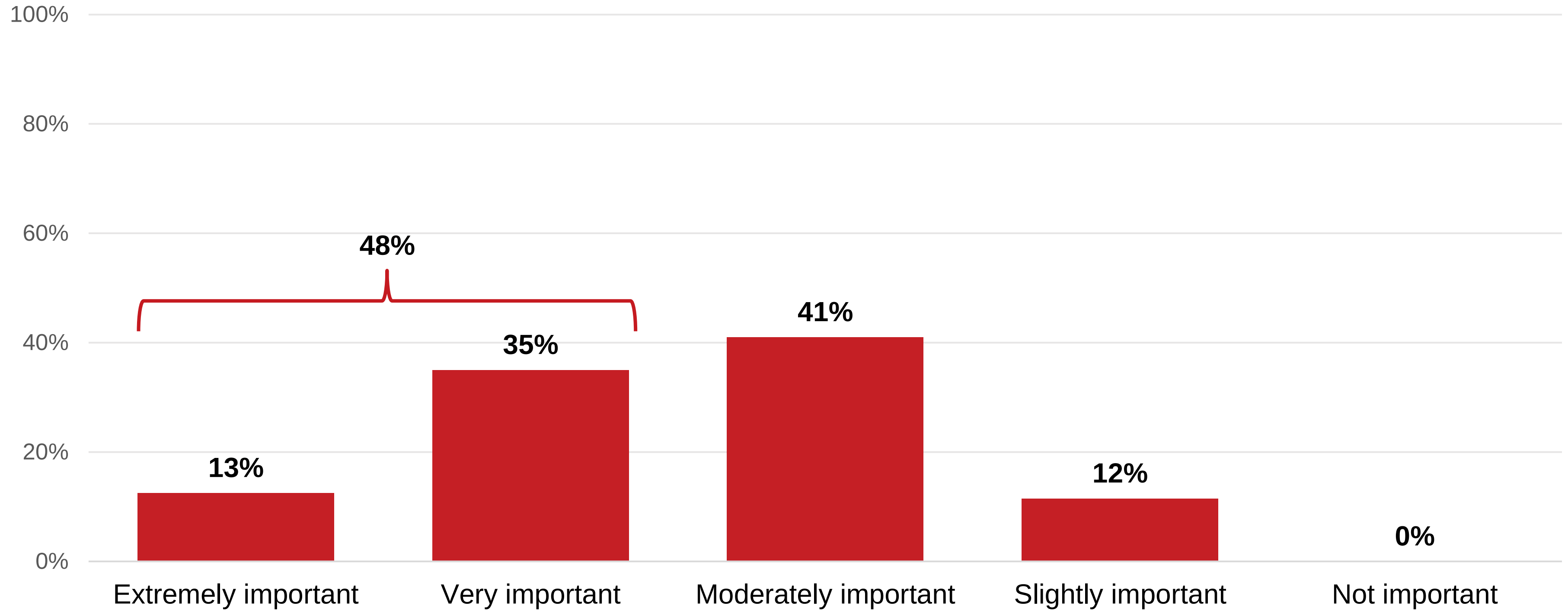
Six in ten indicate that their existing monitoring tools providing visibility into managing hybrid IT environments are moderately effective. Opinions on the effectiveness of current security measures for protecting sensitive data across hybrid IT environments are more divided, with responses split between moderately effective and extremely or very effective.



Q *Currently, how effective are the following in your organization?*

Importance of Observability

Most respondents consider observability important for accelerating digital transformation efforts, with nearly half rating it as extremely or very important.

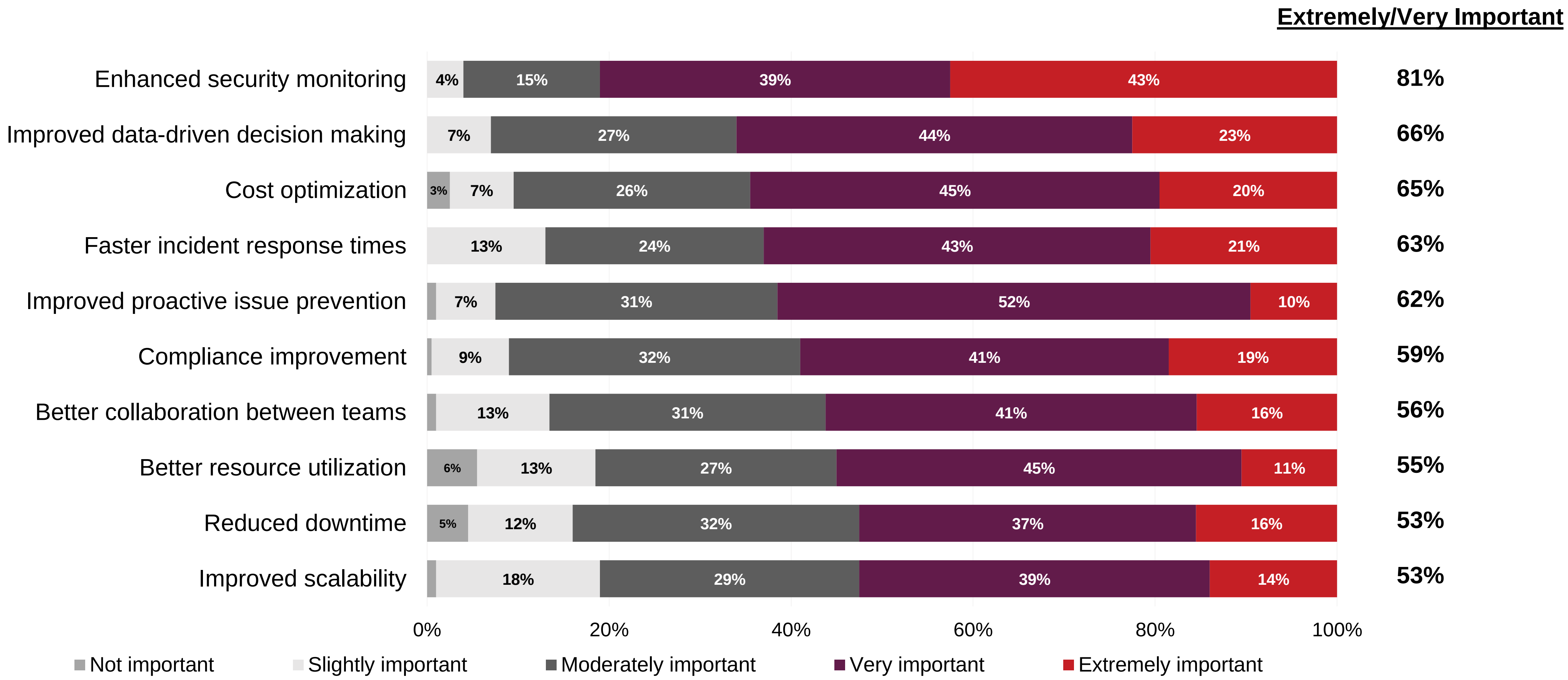


Q *How important is observability in accelerating your organization's digital transformation efforts?*

OBSERVABILITY AND ITS IMPACTS

Benefits of Observability Tools

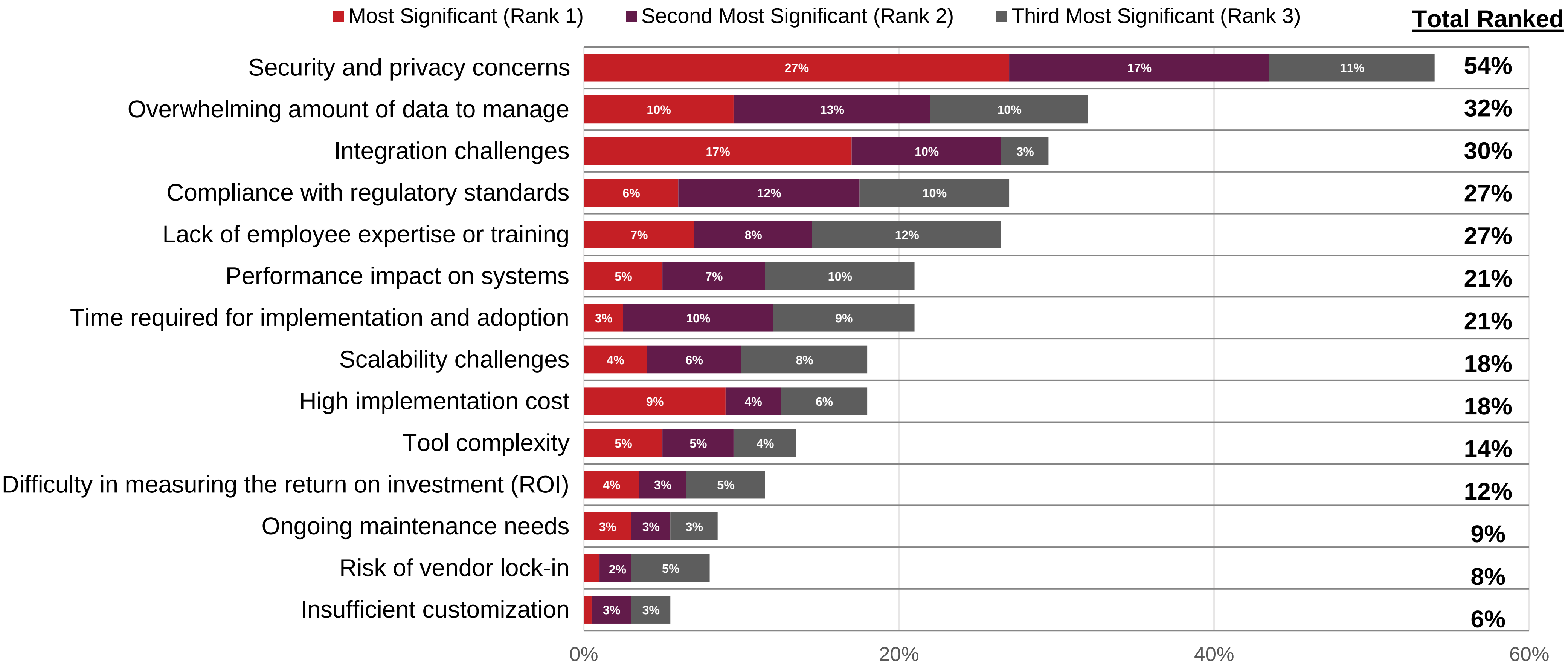
Enhanced security monitoring is the top benefit of implementing observability tools, with eight in ten considering it extremely or very important.



How important are the following potential benefits of implementing observability tools in your organization?

Concerns of Observability Adoption

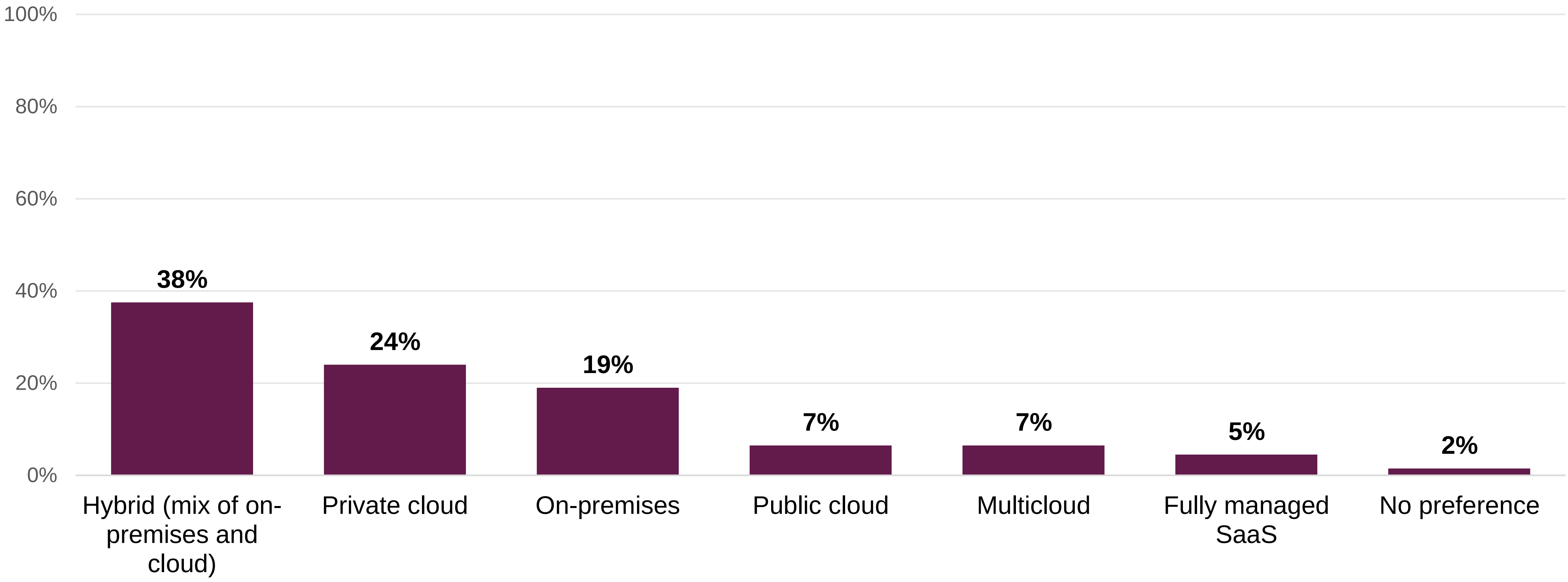
Security and privacy concerns is the top concern regarding the adoption of observability tools, with more than a quarter ranking it as their primary issue.



Q *What are your most significant concerns regarding the adoption of observability tools in your organization? Please rank up to 3 concerns, with #1 being the most significant.*

Preferred Deployment Models

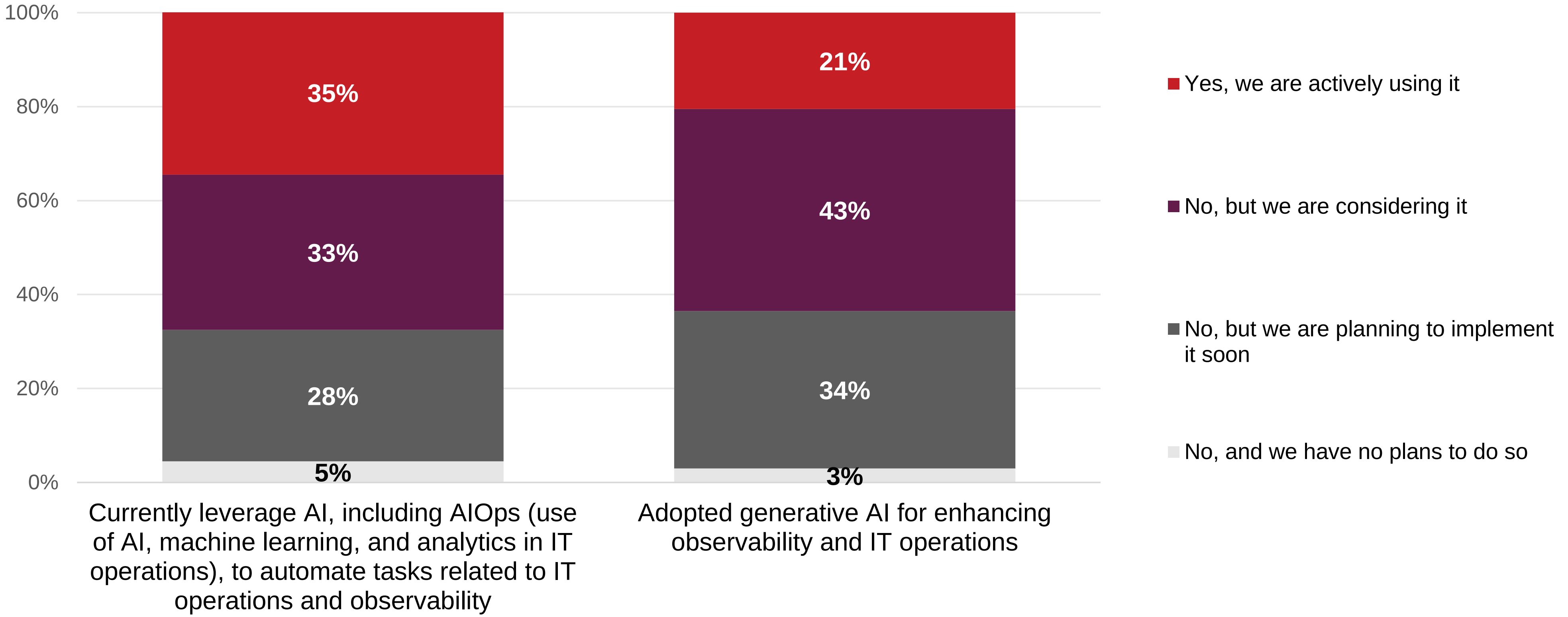
Hybrid is the preferred deployment model for observability solutions, chosen by four in ten, followed by private cloud, preferred by a quarter.



Q *What deployment model for observability solutions is currently most preferred in your organization?*

Leveraging AI

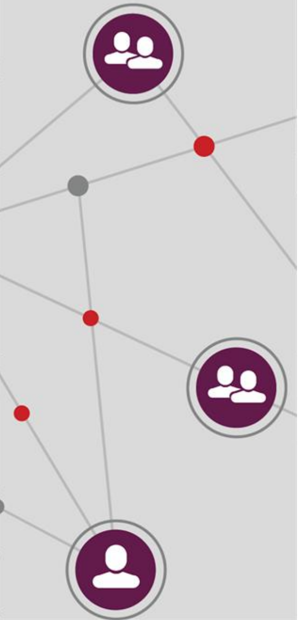
More than a third report currently leveraging AI to automate tasks related to IT operations and observability, while two in ten have adopted generative AI to enhance these areas. Among those who have not, the majority are either considering or planning to implement them soon.

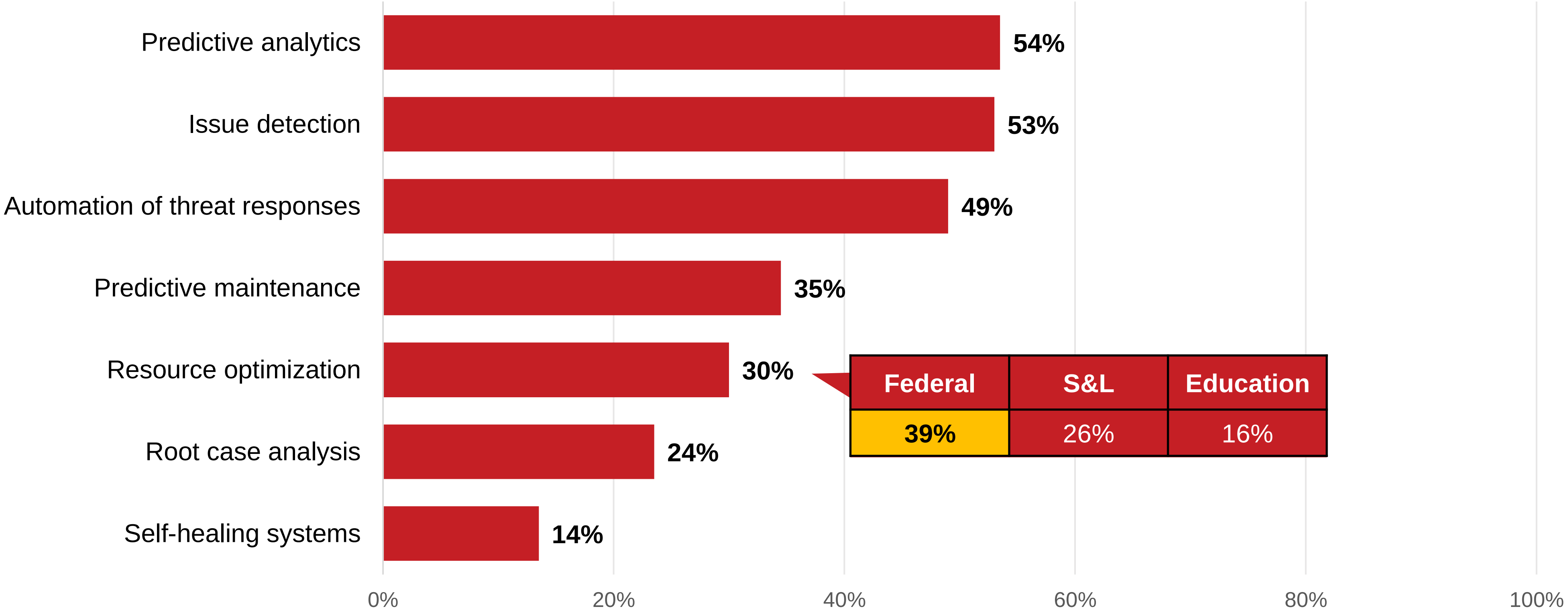


Q *Does your organization currently leverage AI, including AIOps (use of AI, machine learning, and analytics in IT operations), to automate tasks related to IT operations and observability?*
Has your organization adopted generative AI for enhancing observability and IT operations?

Valuable Aspects of AI

Over half of respondents identify predictive analytics and issue detection as the most valuable aspects of AI for improving IT operations.





Federal	S&L	Education
39%	26%	16%

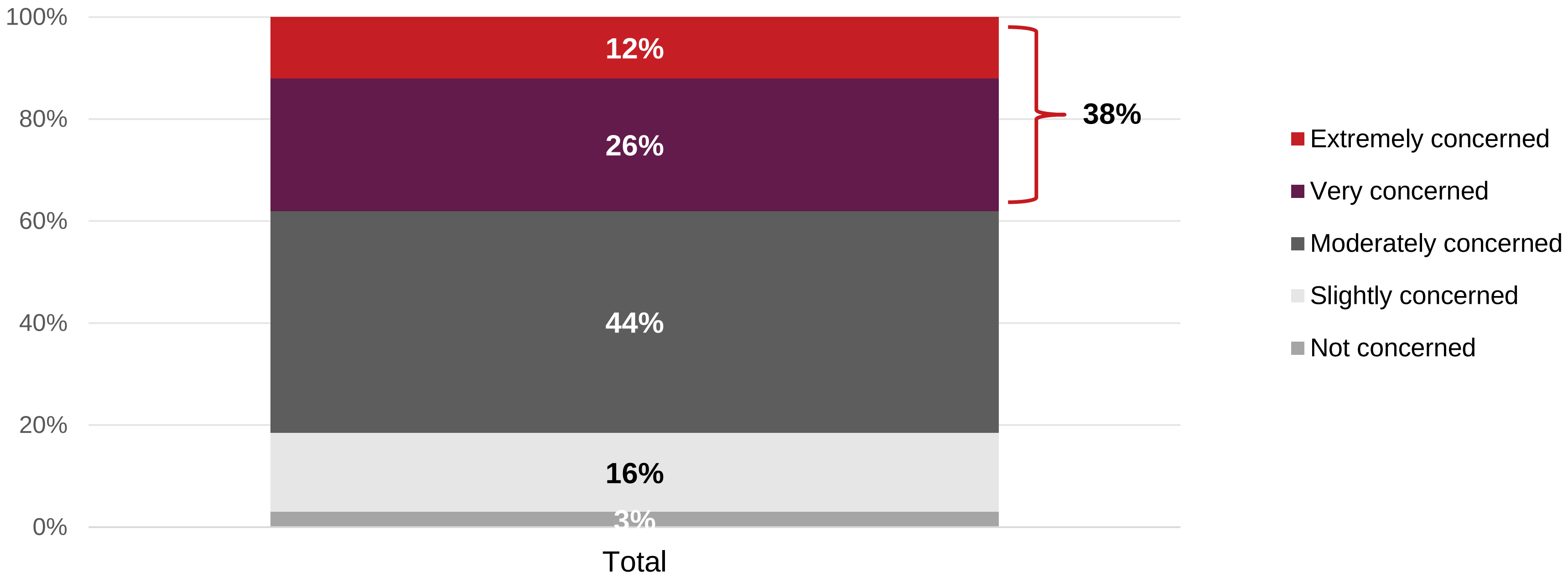
🟨 = significant differences between segments

Note: Multiple responses allowed

Q *What aspects of AI do you find most valuable for improving IT operations? (select up to 3)*

Concerns With AI in IT Management

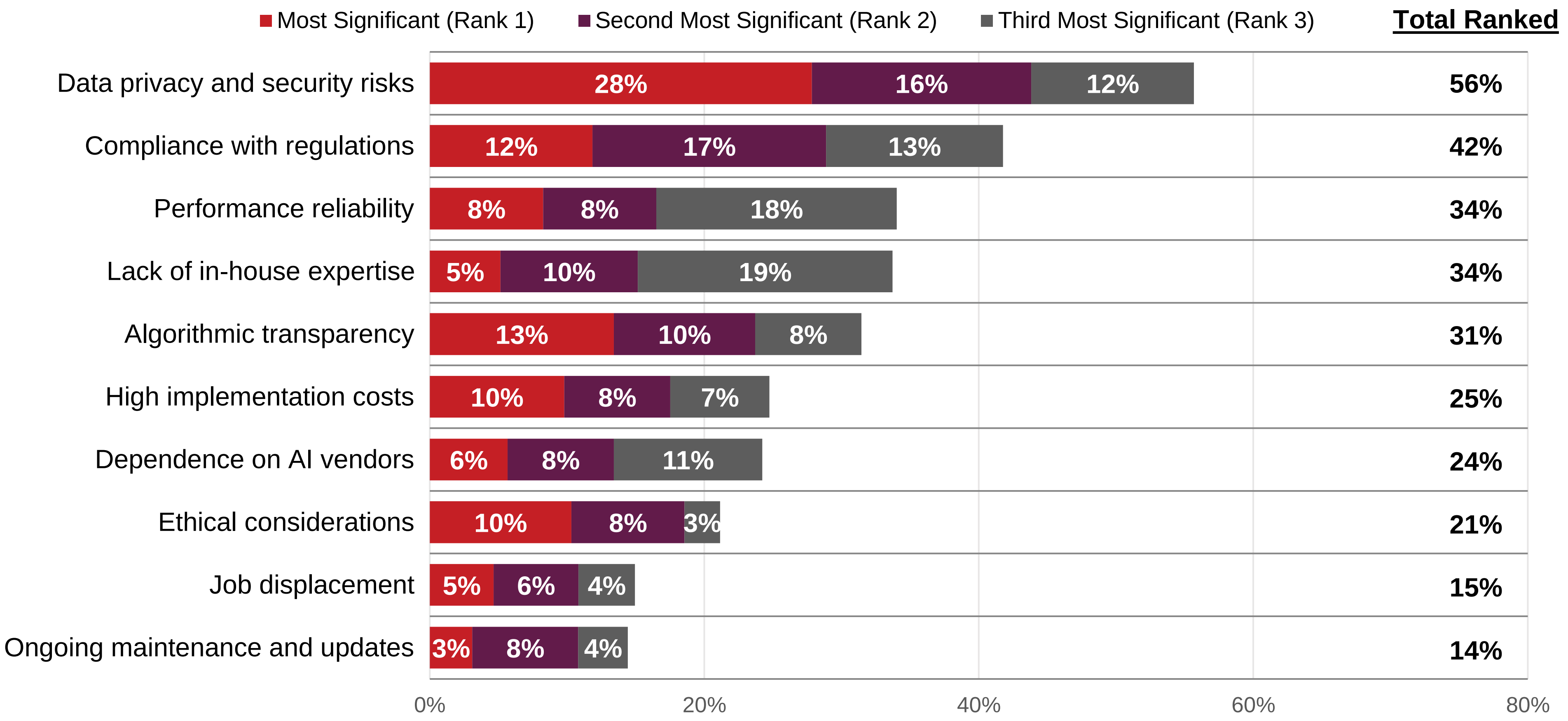
Approximately four in ten are moderately concerned about the potential risks of adopting AI for IT management, while another four in ten are either extremely or very concerned.



How concerned are you about the potential risk associated with adopting AI for IT management?

Risk in AI Adoption

Among those expressing concerns, the top issues with AI adoption are data privacy and security risks, followed by compliance.



	Most Significant (Rank 1)	Second Most Significant (Rank 2)	Third Most Significant (Rank 3)	Total Ranked
Data privacy and security risks	28%	16%	12%	56%
Compliance with regulations	12%	17%	13%	42%
Performance reliability	8%	8%	18%	34%
Lack of in-house expertise	5%	10%	19%	34%
Algorithmic transparency	13%	10%	8%	31%
High implementation costs	10%	8%	7%	25%
Dependence on AI vendors	6%	8%	11%	24%
Ethical considerations	10%	8%	3%	21%
Job displacement	5%	6%	4%	15%
Ongoing maintenance and updates	3%	8%	4%	14%

Q *[SKIP IF NOT CONCERNED IN PREVIOUS QUESTION] What are your most significant concerns regarding the risks associated with adopting AI for IT management? Please rank up to 3 concerns, with #1 being the most significant.*

Elizabeth Lowery, Director of Research Services

elowery@govexec.com

Julia Hagen, Research Analyst

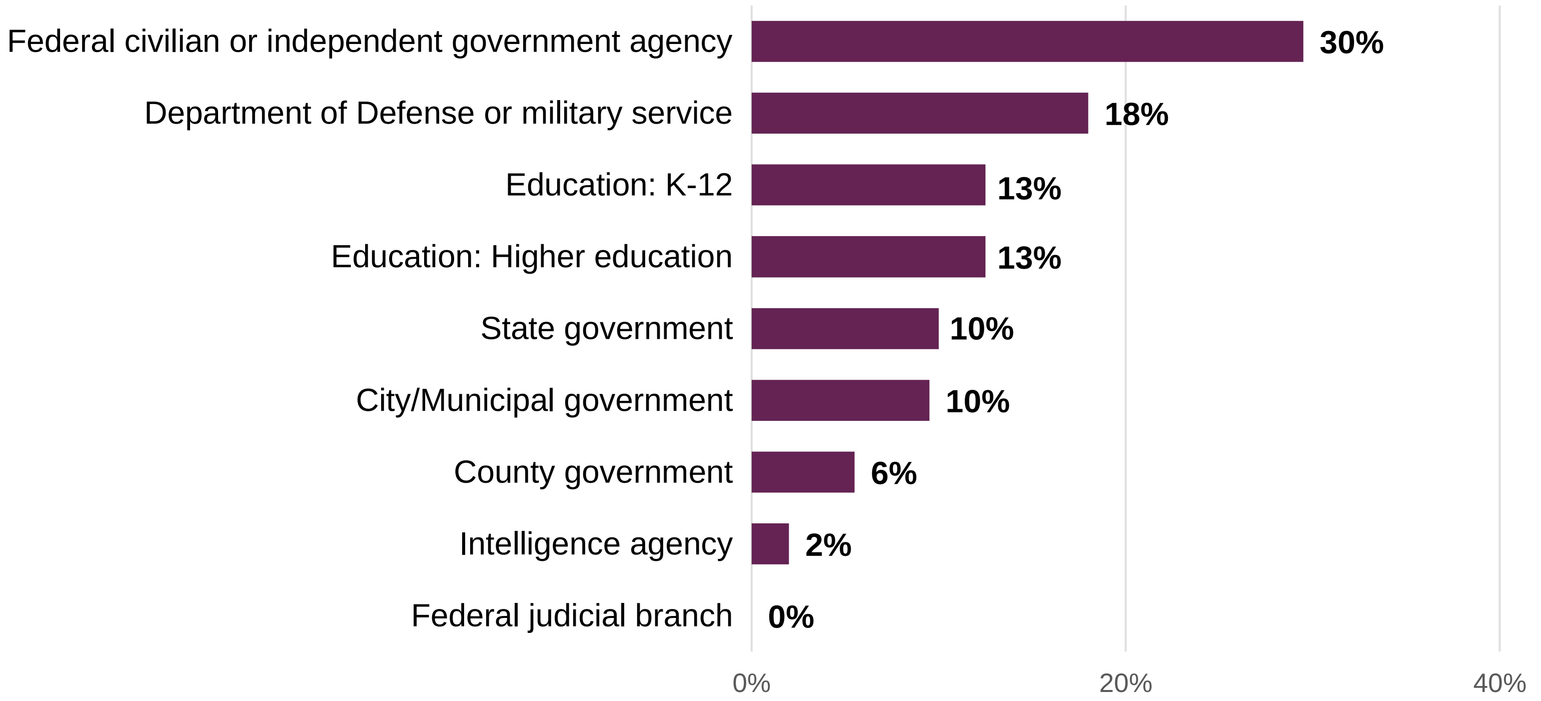
jhagen@govexec.com

Appendix:
Respondent Classifications

Organizations Represented

A wide array of organizations are represented, and respondents are evenly split between federal and SLED organizations.

Organization Type



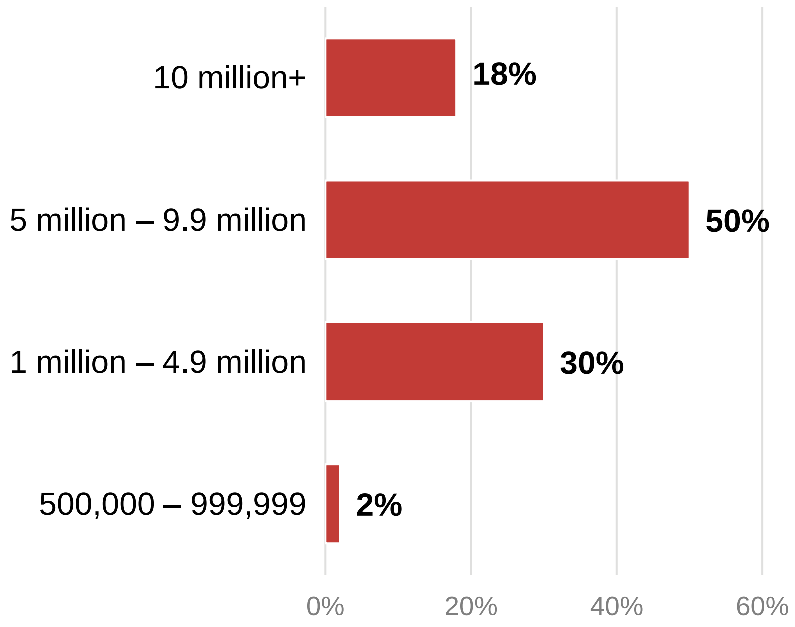
	Count	Percent
Federal Government	100	50%
State and Local	50	25%
Education	50	25%

Which of the following best describes your current employer?

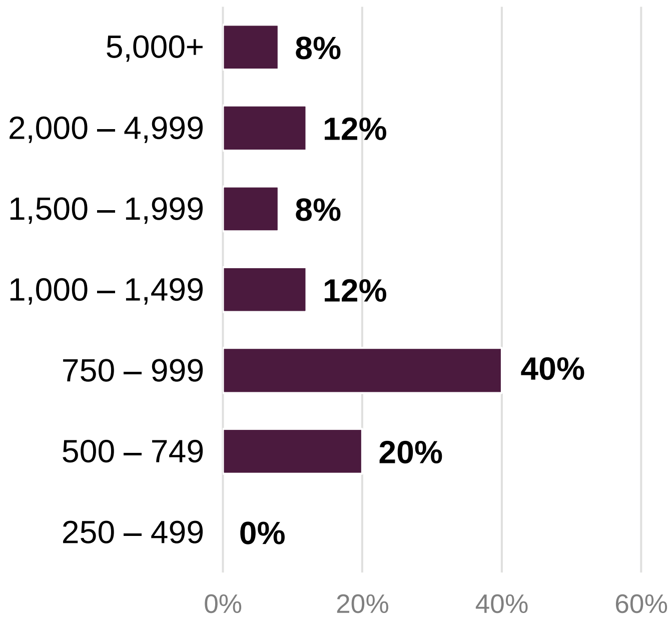
SLED Population and Enrollment

Respondents were screened to ensure they met minimum population and enrollment thresholds.

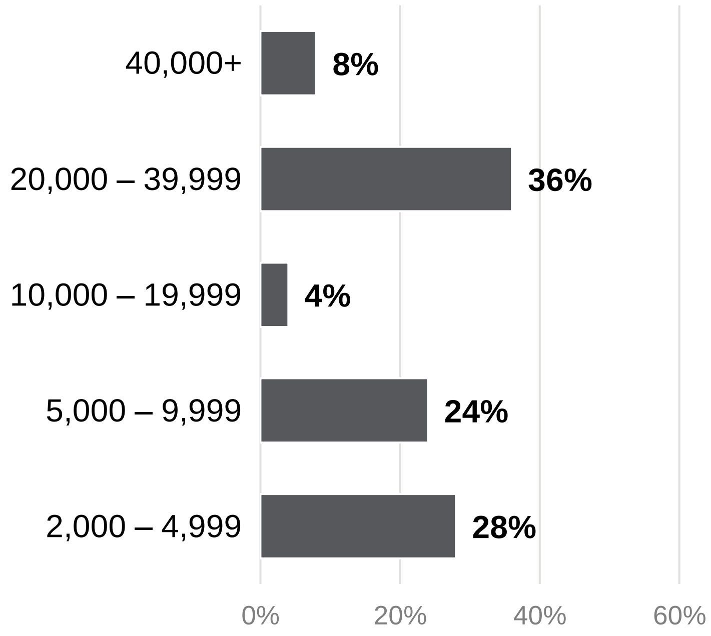
State and Local Population



K-12 Enrollment*



Higher Education Enrollment*

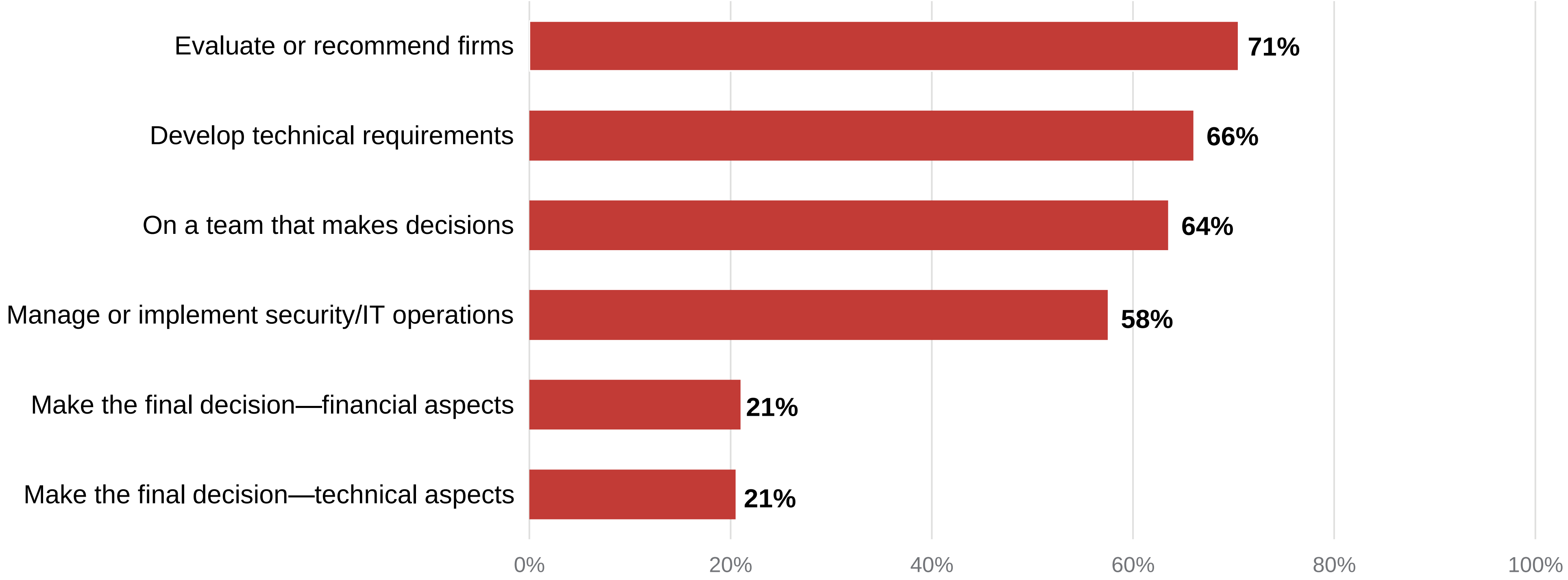


*Small sample size

[STATE, COUNTY, OR CITY GOVERNMENT] What is the estimated population of the [“state”, “county,” OR “city”] that you work for?
[EDUCATION: K-12] How many total students are currently enrolled at the school(s) where you are involved with IT security and/or IT operations and management?
[EDUCATION: HIGHER EDUCATION] How many students are currently enrolled at your college or university?

Decision-Making Involvement

Respondents were screened to ensure they are involved in IT operations and management and IT security solutions and services in their organization.

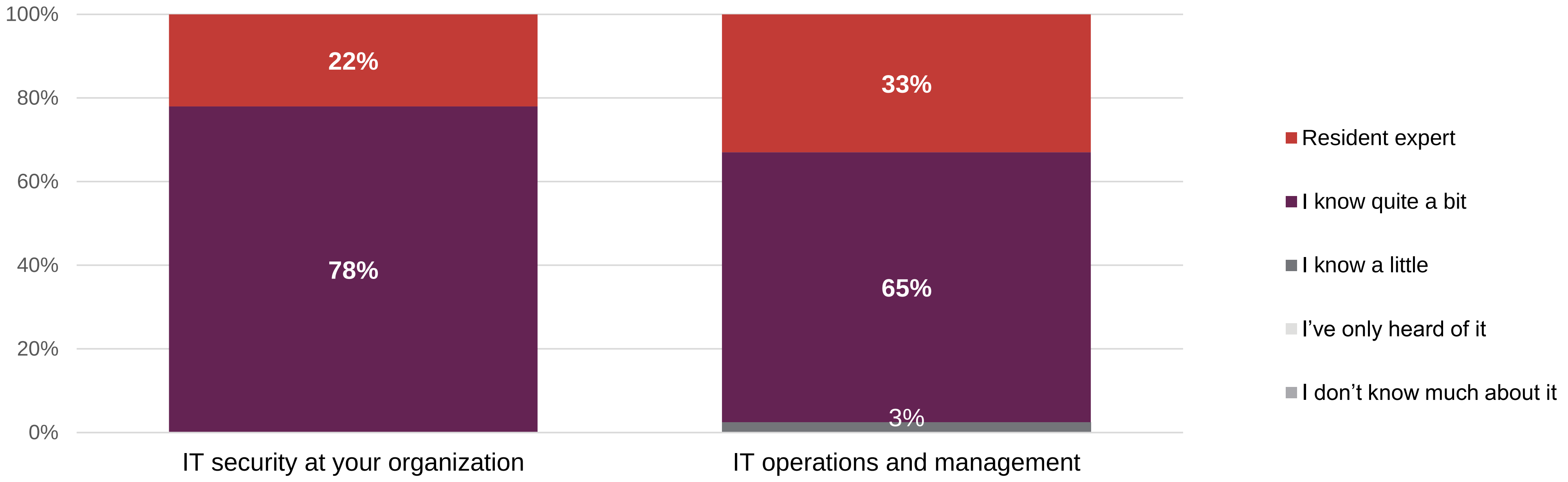


Note: Multiple responses allowed

Q *How are you involved in your organization's decisions or recommendations regarding IT operations and management and IT security solutions and services? (select all that apply)*

Familiarity With IT

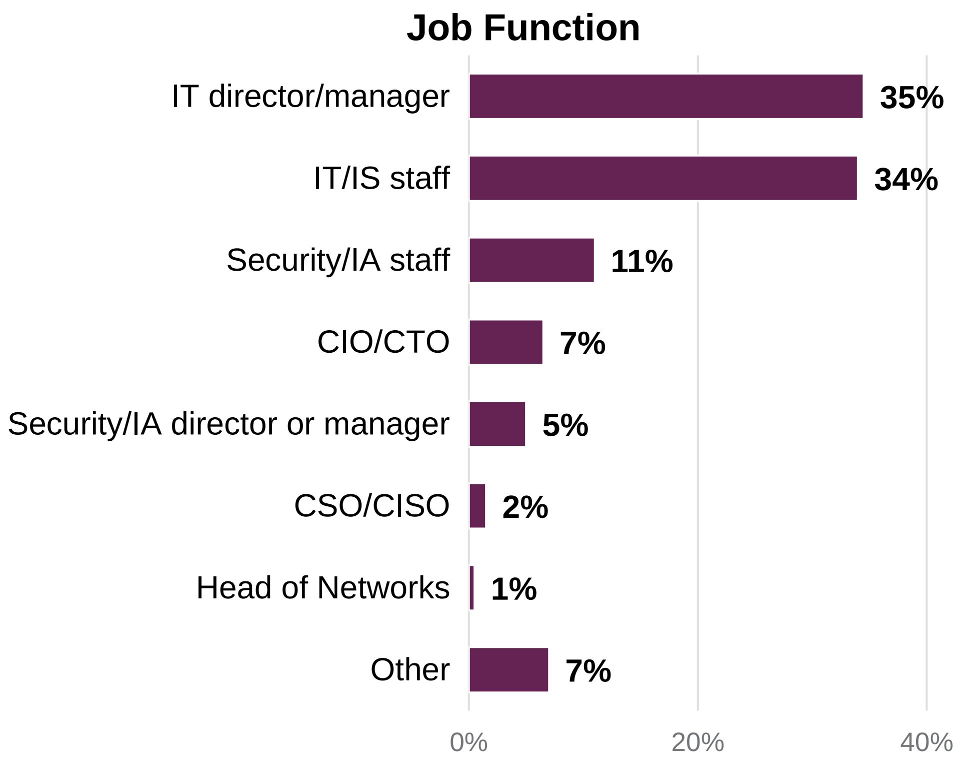
Respondents were required to be familiar with their organization's IT security and IT operations and management.

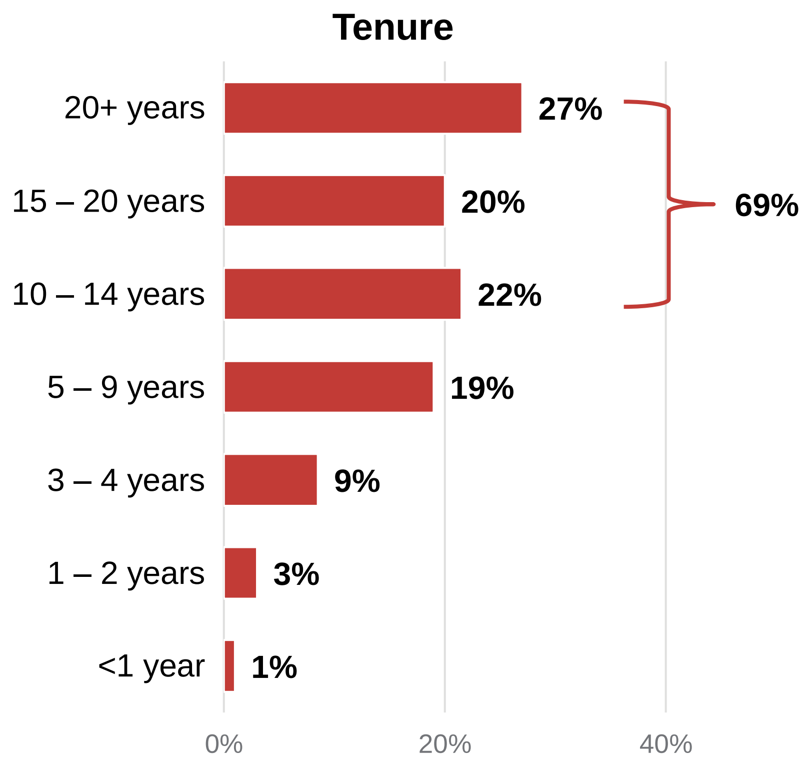


How would you describe your familiarity with:

Job Function and Tenure

Seven in ten are IT directors and managers or IT and IS staff and have worked in the public sector for a decade or more.

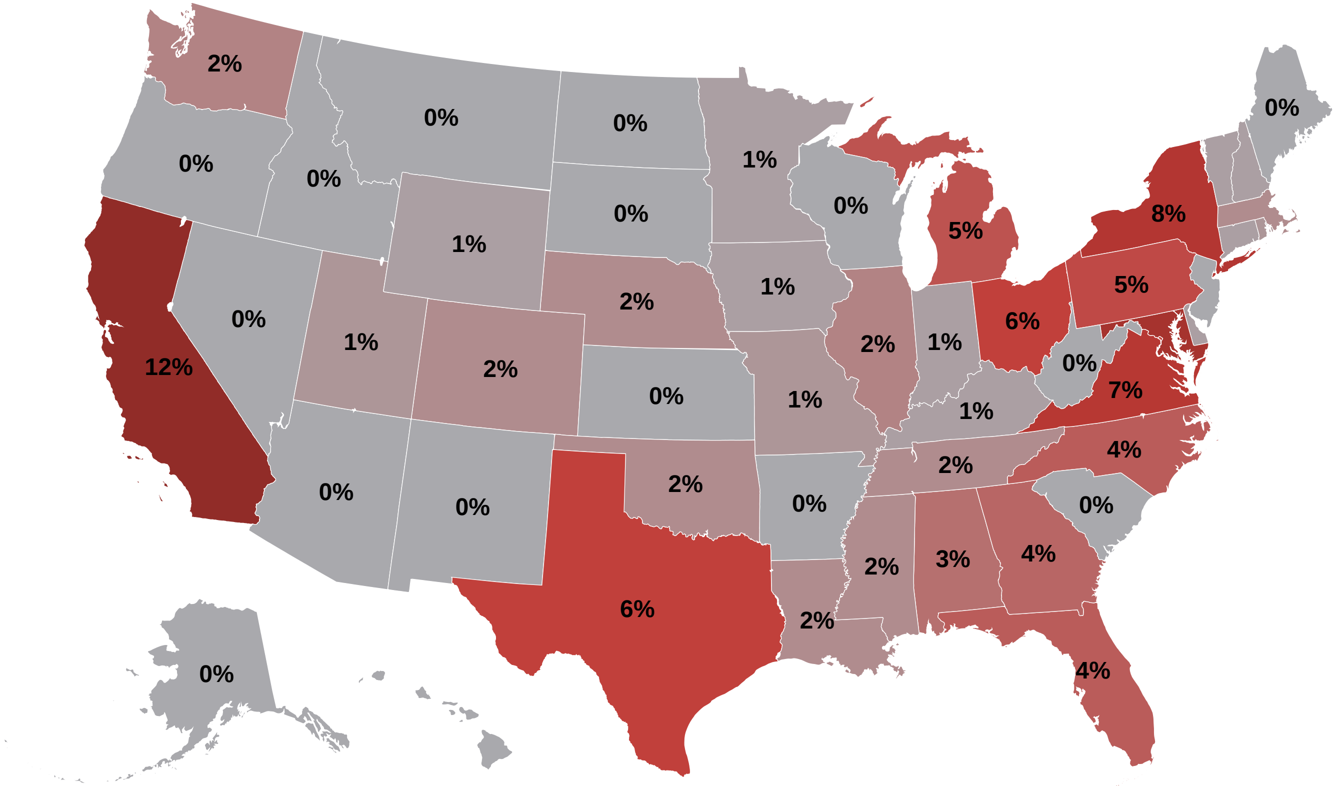




Which of the following best describes your current job title/function? How long have you worked in the Public Sector?

States Represented

Respondents come from various states with larger proportions from California, Maryland, New York, and Virginia.



What state do you currently work in?