Omada

The State of Identity Governance 2025

Contents

Executive Summary

To understand the current landscape of identity governance in large organizations, Omada surveyed over 500 IT and business leaders. The survey included professionals responsible for identity governance, access management, compliance, cybersecurity, and overall IT administration, providing valuable insights into the state of IGA in 2025.

The research reveals:

- **Organizations are spending more on cybersecurity:** Nine out of 10 respondents said the teams/ resources responsible for IT security in their organizations are better funded than they were a year ago. At the same time, more than 6 in 10 (64.4%) respondents said they've purchased cyber liability insurance to help offset the costs of a data breach.
- **Organizations still struggle with their IGA investments:** Nearly four in 10 organizations still haven't deployed SaaS-based IGA, even though they recognize the need for a modern solution. What's more, nearly 60% of respondents identified restrictive total cost of ownership (TCO) as a principal deficiency in their current IGA solution.
- **AI and automation are top criteria when choosing IGA solutions:** More than half of respondents cited time-consuming manual processes as either the first or second issue driving their organization's IGA investment. As a result, AI and automation are key attributes that leaders look for when evaluating potential solutions, with Generative AI capabilities emerging as a top criterion.

Key Findings from The State of Identity Governance 2025

Investment in IT Security Continues to Grow
IT security spending is on the rise, with nearly 90% of respondents reporting increased funding for their security teams and resources over the past year. This trend reflects the growing importance of cybersecurity in today's business landscape.

Organizations may be spending more on IT security in part to keep pace with proportionally higher monetary losses because of data breaches, particularly in industries that maintain large volumes of sensitive data. For example, the International Monetary Fund* reported that the size of financial losses from cybersecurity incidents in the financial sector has more than quadrupled since 2017 to US$2.5 billion. Also, the data suggests that most organizations have clear ideas about what capabilities they need to improve and how these improvements will affect process efficiency and return on investment.

Cyber Liability Insurance is Gaining Traction
As the cost of data breaches rises, many organizations are turning to Cyber Liability Insurance. More than six in ten respondents (64.4%) said their organizations are investing in Cyber Liability Insurance to offset the cost of a data breach. Given the rise in financial losses tied to data breaches, this trend is understandable. Still, recent findings from Network Assured** indicate that only 19% of businesses have coverage for security incidents exceeding $600,000 USD. With the average ransom paid by breached organizations topping $800,000 USD, many businesses may find themselves underinsured. To address these risks, insurers increasingly require stronger cybersecurity measures, including enhanced access controls, robust authentication protocols and a well-defined identity governance program – actions that all demonstrates an organization's commitment to meeting insurers' security requirements.

The need for improved efficiency drives IGA Investment
Time consuming manual processes and complex access governance are the key business issues driving IGA investment.

Over six in ten (61.2%) respondents cited time consuming manual processes as either the top or second-to-the-top issue driving their organization's IGA investment. This suggests that for most organizations, identity lifecycle management and error-prone manual onboarding, offboarding, user access management are ongoing challenges. Also, more than six in ten (64.4%) respondents report that complex access governance, the cumbersome process of managing user permissions across various systems is a top or second-to-the-top issue they are looking to solve with investment in IGA solutions.

Citations for external references
*The IMF Reference "Rising Cyber Threats Pose Serious Concerns for Financial Stability", IMF Blog, 9 April 2024
https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

**Network Assured Reference "23 Eye-Opening Cybersecurity Insurance Statistics", Network Assured Blog, 7 August 2024
https://networkassured.com/security/cybersecurity-insurance-statistics/

IGA Challenges Highlight the Need for More Efficient Solutions

Organizations face significant barriers with current IGA solutions, including high total cost of ownership (TCO), complex customization needs, and difficulties in ensuring appropriate user access control. These deficiencies are prompting the demand for more efficient and flexible IGA solutions.

Nearly 60% of respondents identified restrictive TCO as a principal deficiency in their current IGA solution. This suggests they are finding that making upgrades to the existing solution is too time-consuming or requires resources that are not available. More than half said that the development effort and skills required to support the IGA solution with customization is a significant gap. Nearly 46% claim that difficulty ensuring users have appropriate level of access to systems and data and an inability to automate access control and compare access rights are existing functionality gaps in their current IGA solution.

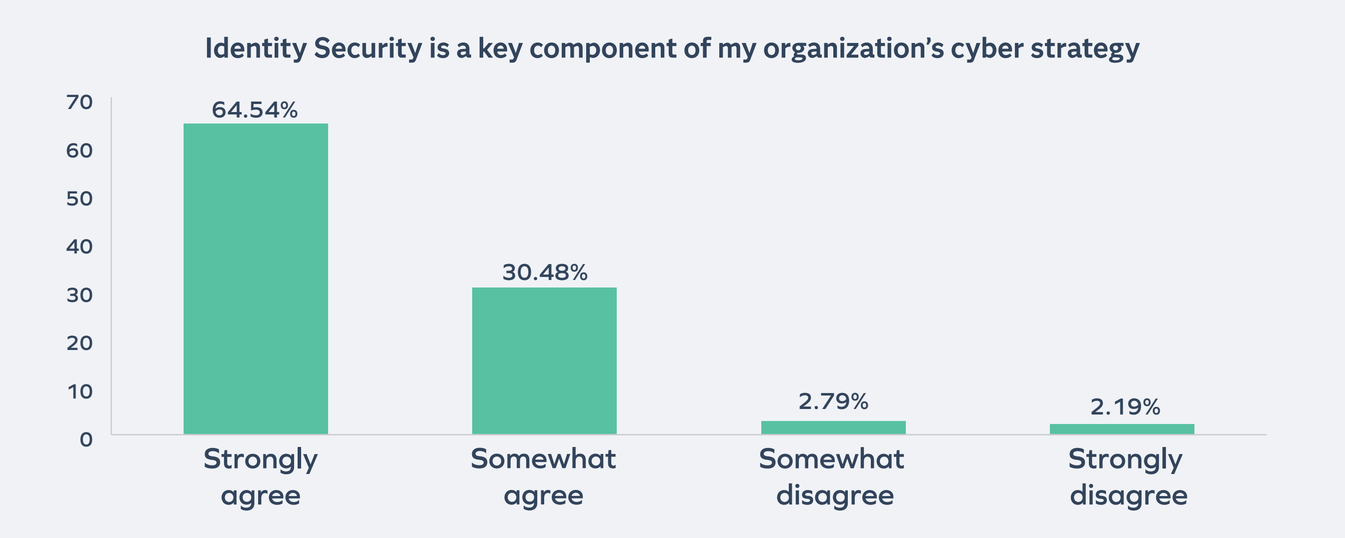
Improving ROI with Advanced IGA Features

Role-based Access Control (RBAC), enhanced access visibility, and user behavior insights are essential features that can significantly boost the return on investment (ROI) for IGA solutions. Cloud-based platforms offering these capabilities are particularly beneficial for modern businesses.

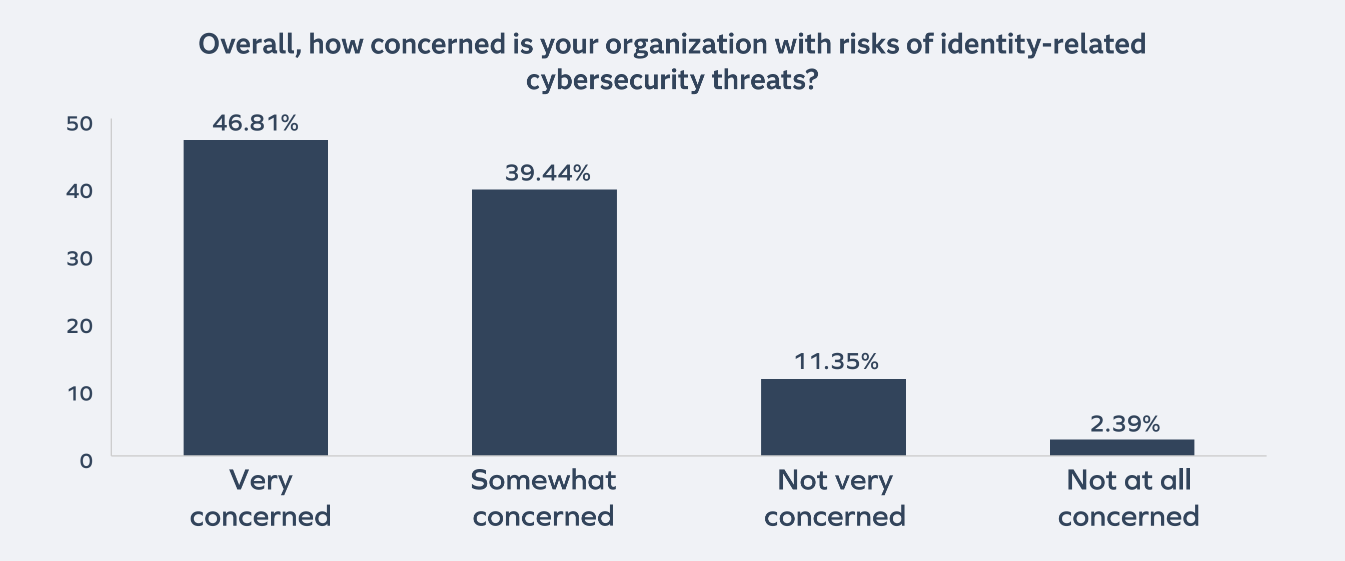
When asked what features would increase their organization’s return on its IGA investment most, 56.8% of respondents cited cloud-based user access control like RBAC. These findings suggest that many organizations would gain significant bottom-line benefits from adopting a cloud-based IGA solution that enables enhanced access control across on-premises, cloud, multi-cloud, and hybrid environments.

The Current State of Identity Security

Most respondents said that identity security is a priority for their organizations and their security teams are getting more funding. At the same time, concerns about identity-related cybersecurity risks appear slightly less urgent than last year.

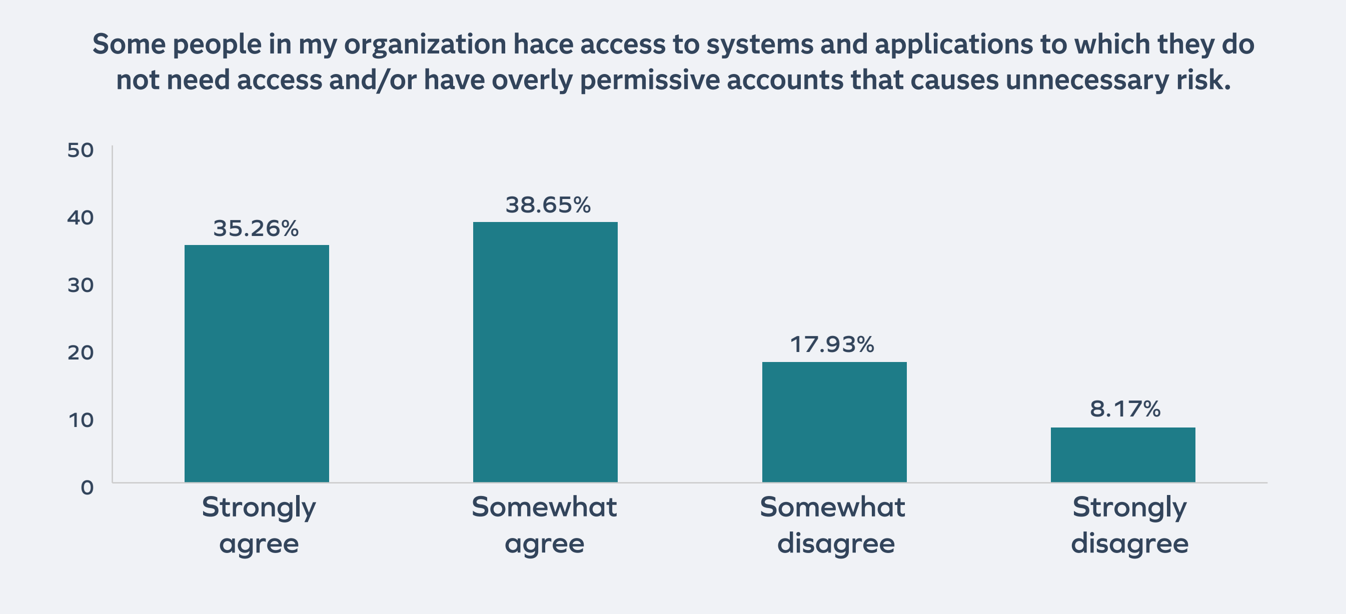


An overwhelming majority (95%) of survey respondents agree that identity security is a key component of their organization’s cybersecurity strategy, with 64.5% said they strongly agree.



More than 86% of IT professionals and business leaders surveyed admitted that their organizations are concerned about the risks of identity-related security threats, with 46.8% said they are very concerned. In *The State of Identity Governance 2024*, over 90% of respondents said they were concerned about these risks, with 61.4% said last year that they were very concerned.

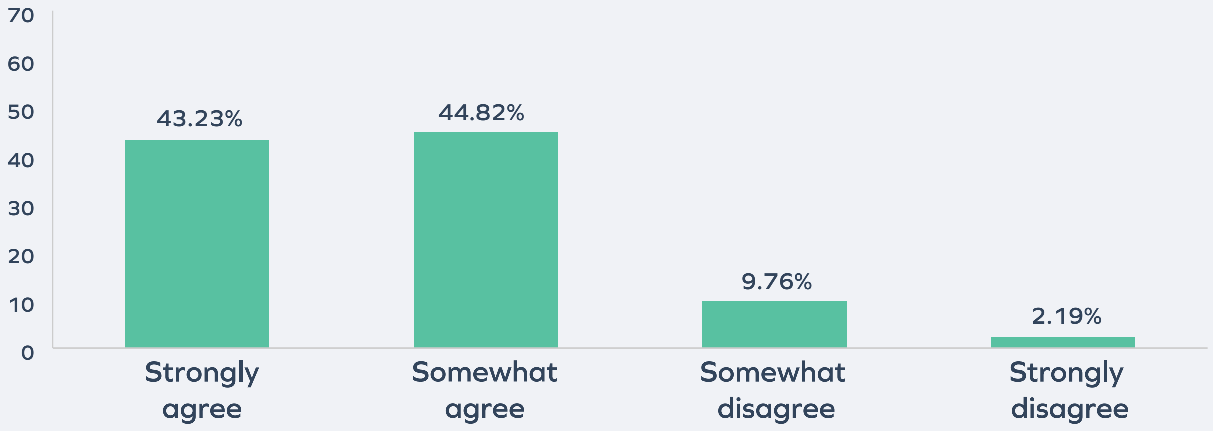
Excessive access permissions remain a concern for IT and business leaders



The Survey reveals that 73.9% of respondents strongly or somewhat agree that people in their organizations have access to systems and applications they don't require, and these overly permissive accounts cause unnecessary risk. This is slightly higher than respondents reported in *The State of Identity Governance 2024* (70.9%) and may suggest that the previously mentioned gaps in current IGA solutions are contributing to a lack of more effective user access control and leaving more people over-permissioned.

More than eight in ten respondents agree their organization's core security competencies are sufficient in identifying anomalous user behavior in real-time, allowing organizations to act and adapt accordingly.

My organization's detection and response system easily identifies risky or anomalous user behavior in real time and takes action (e.g., locking a suspicious account).

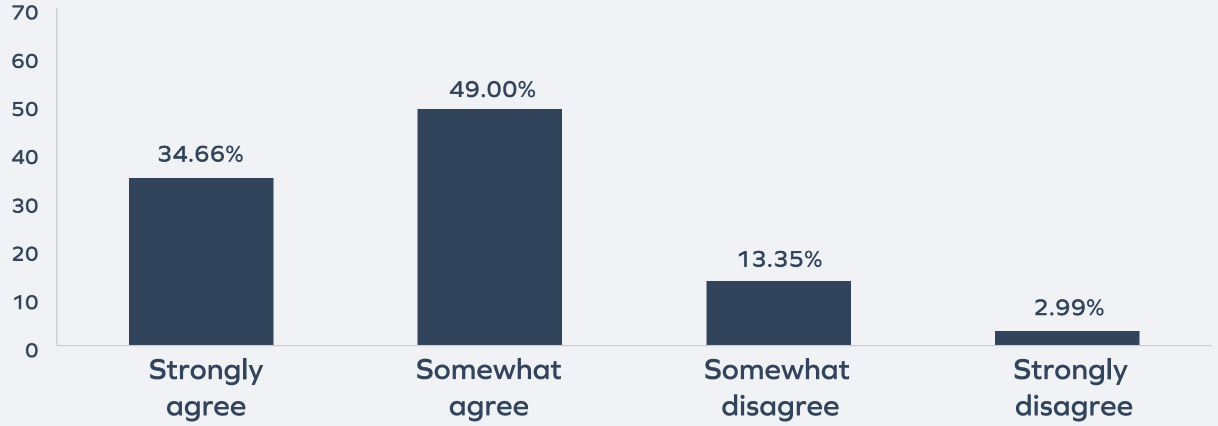


Despite reporting gaps and deficiencies in their organizations IGA systems, respondents remain confident in their ability to perform critical security capabilities such as identifying anomalous user behavior (89%), adapting to new business conditions (83.7%), and compliance reporting (85.3%). However, over 70% of respondents report that some users have unnecessary access to their IT infrastructure, underscoring the gap between confidence in these core competencies and the ongoing risk of overly permissive access. While many organizations believe they effectively detect threats and respond to evolving requirements, the ongoing issue of overly permissive access shows that tightening access controls to reduce unnecessary risk remains a challenge.

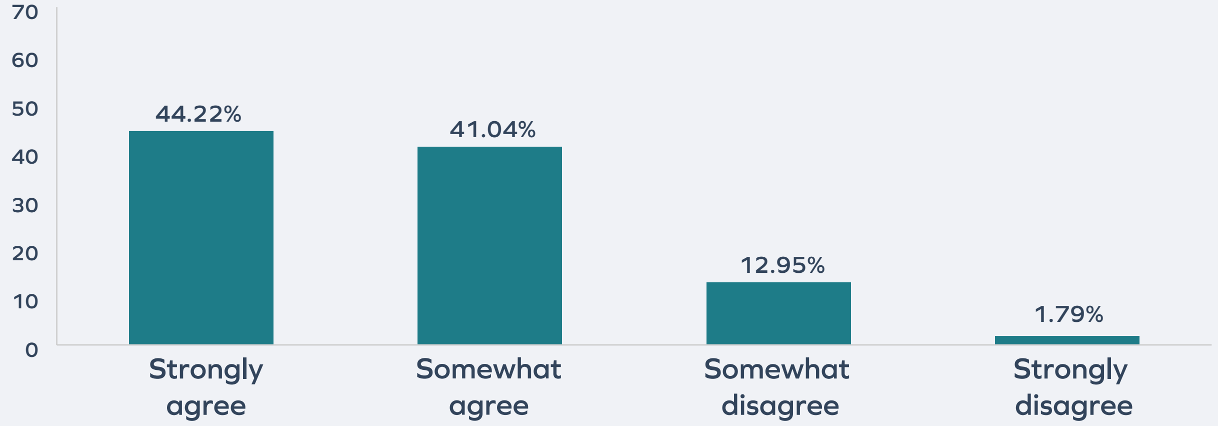
Efficiency and Regulatory Compliance

Efficiency plays a key role in how organizations manage access and maintain compliance across ever-evolving regulatory environments. With data privacy and industry-specific mandates intensifying, many businesses are prioritizing automated identity lifecycle management to replace time-consuming manual processes.

My organization's identity management easily adapts to new business requirments (e.g., new systems, shifting resources, M&A, cloud-hosted environments, etc.).



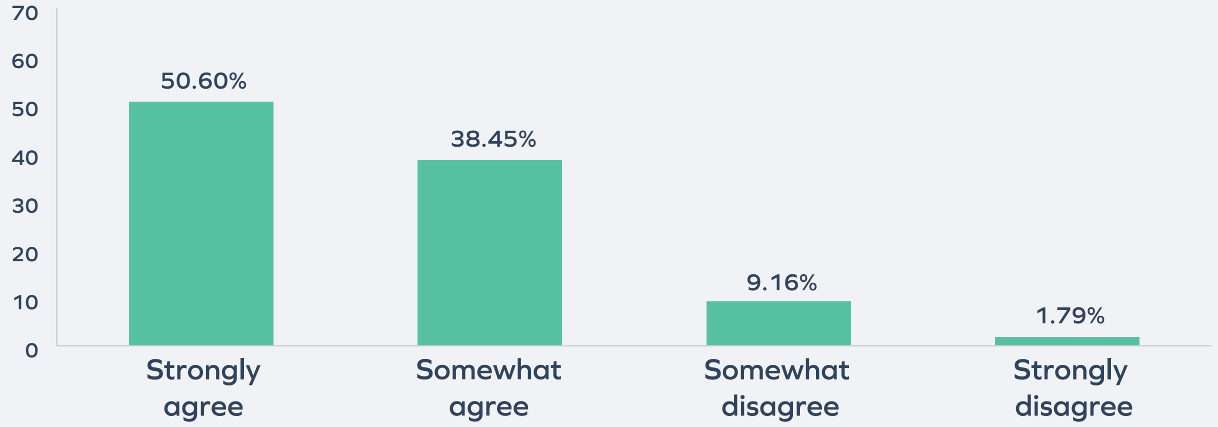
My organization's identity governance software makes it easy to create regulation-specific reports that are necessary to comply with industry regulations and data protection laws, such as GDPR or HIPAA/HITECH.



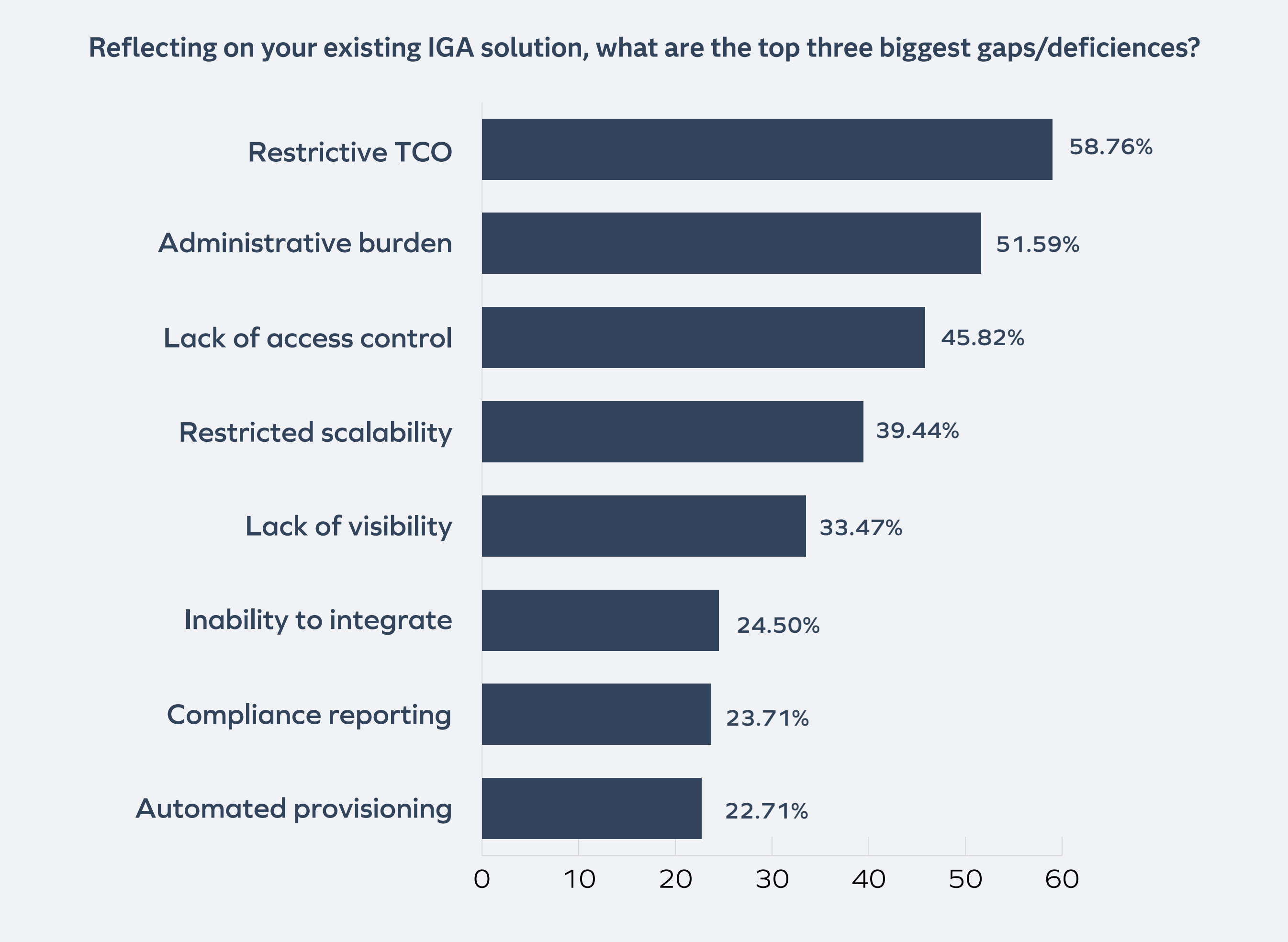
Key Drivers for IGA Investment

Inability to automate critical IGA processes such as identity lifecycle management is widely seen as a deficiency in current IGA solutions and bridging this gap is driving IGA investment.

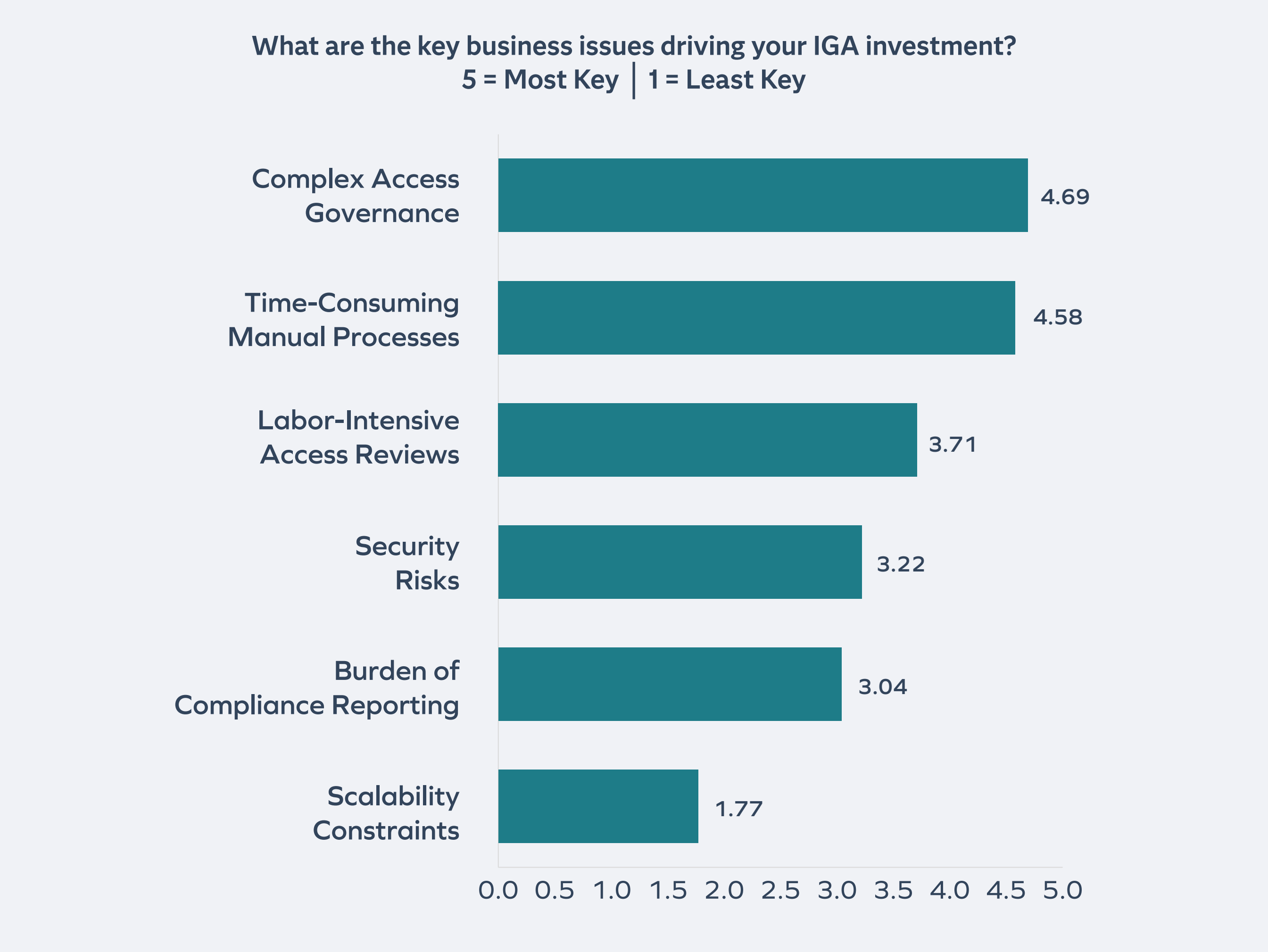
Teams and resources for IT security in my organization are better funded today than a year ago.



When asked if their IT teams and resources are better funded than they were in the prior year, 89% of survey respondents said they were; with more than half reporting they strongly agree their teams are better funded.



Time-consuming upgrades and complex customization to existing IGA solutions that restrict TCO (58.8%), the burden of marshaling the skills and administering development efforts to support their existing solutions (51.6%), and difficulty in automating access control and comparing access rights and accounts in their current state to their desired state to ensure users have the appropriate accessto systems and data (45.8%) are cited by respondents as the three biggest gaps in their capacity to manage identity security effectively.



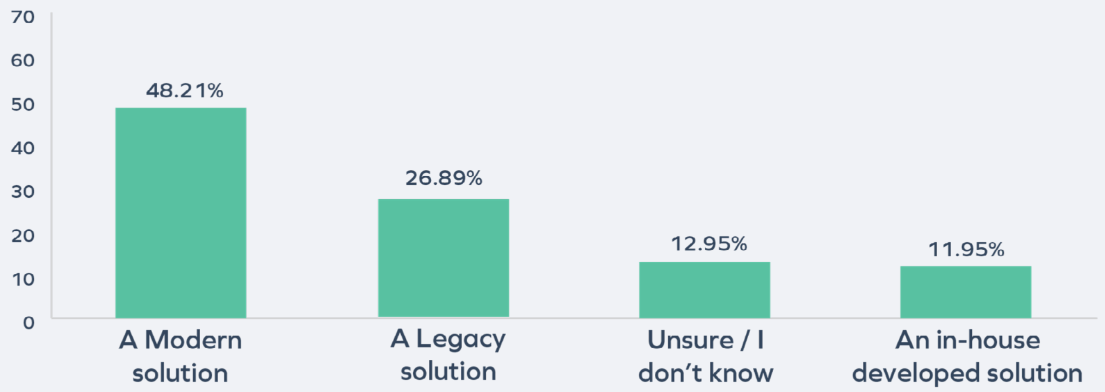
The key issues driving IGA investment in respondents' organizations align with the aforementioned deficiencies in existing IGA solutions. As managing user permissions across various systems is cumbersome and prone to errors that lead to delays and potential security risks, respondents identified the capacity for complex access governance as the top business driver of their IGA investment. Acquiring the capacity to automate identity lifecycle management and make the manual process of onboarding, offboarding, and managing user access more efficient was also considered by respondents to be a top driver of IGA investment.

Staying Competitive: The Need for Cloud-based and AI-driven IGA Solutions

Despite a growing need to automate IGA functionalities and create more efficiency, nearly four in ten organizations still have not deployed SaaS-based modern IGA solutions.

Organizations recognize the need to improve IGA through modern approaches—such as shifting to cloud-based solutions and incorporating generative AI—many remain tethered to legacy or homegrown systems. This suggests an environment ripe for change: the most impactful improvements, like more intuitive role-based access control and better user behavior insights, may only be realized after a deliberate move away from older, complex setups. Such a shift could reduce overall TCO by cutting down on manual processes, complex customizations, and time-consuming upgrades.

What type of Identity Governance and Administration (IGA) solution does your organization currently use?

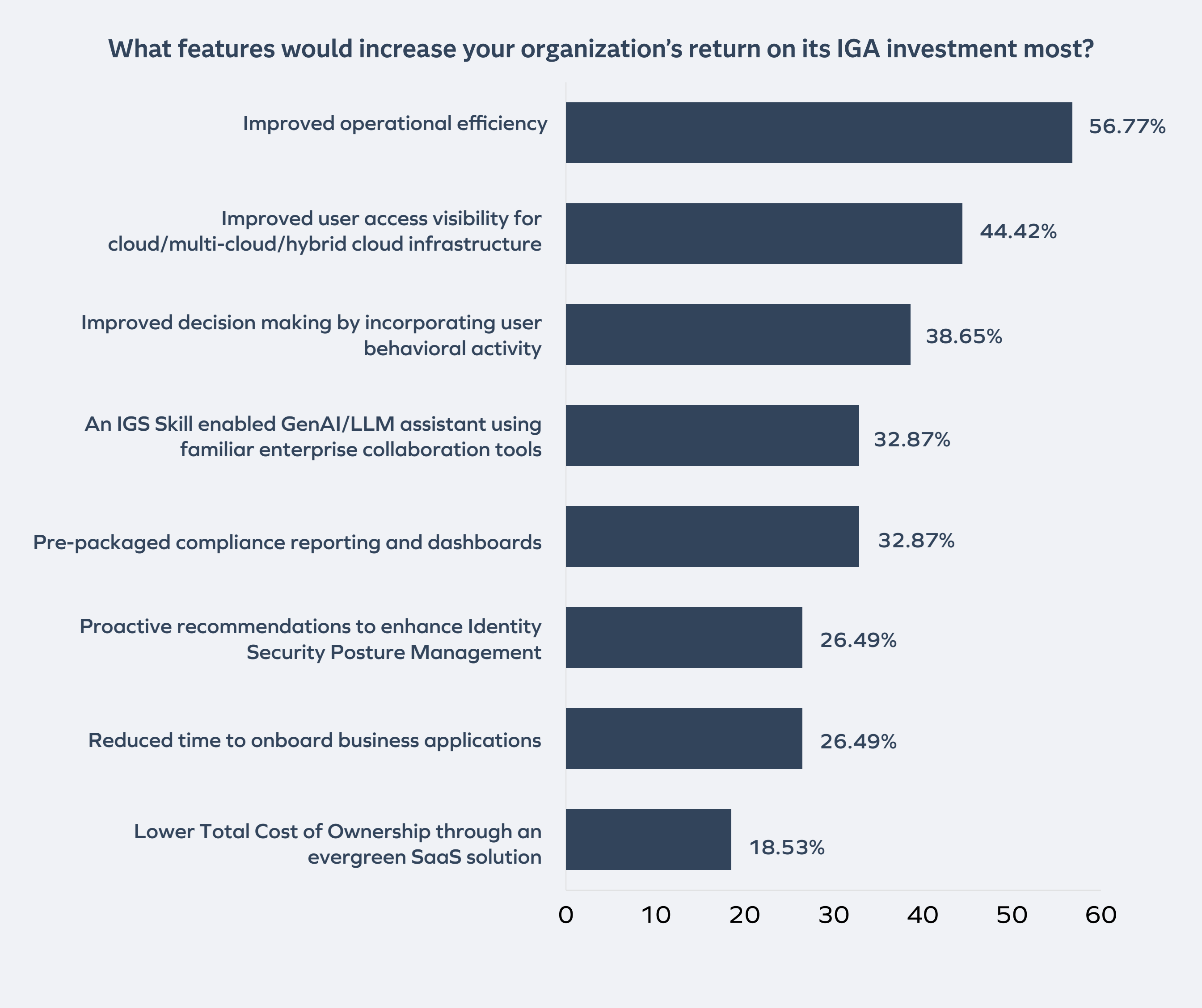


Today, 26.9% of respondents report that their organizations still use legacy IGA solutions that do not support modern authentication open standards, with another 12% still using in-house developed IGA solutions. This data is not dramatically different from that reported in *The State of Identity Governance* 2024 in which 27.3% of respondents said that were using legacy IGA and 14.8% were using a "homegrown" IGA system.

There were, however, some notable differences in Survey responses from people using legacy or in-house developed IGA systems versus those using modern IGA solutions. 22.9% more respondents using legacy and in-house developed solutions identified managing inefficient manual onboarding, offboarding, and user access as key business issue driving IGA investment than their counterparts using modern SaaS-based solutions. 23.5% more said improving user access visibility for cloud/multi-cloud/hybrid cloud infrastructures would be a key feature in increasing their organizations' ROI on IGA investment. 20.9% more identified a SaaS-based service as a key characteristic they look for when evaluating a new IGA solution. 17.7% more agreed that people in their organization had excessive privileges access causing unnecessary risk.

The Future of IGA: Trends to Watch

Cloud-based Role-Based Access Control (RBAC) Discovery, improved user access visibility in cloud infrastructures, and improved decision making with user behavioral activity top the “wish list” of features that would deliver the best ROI on IGA investment.

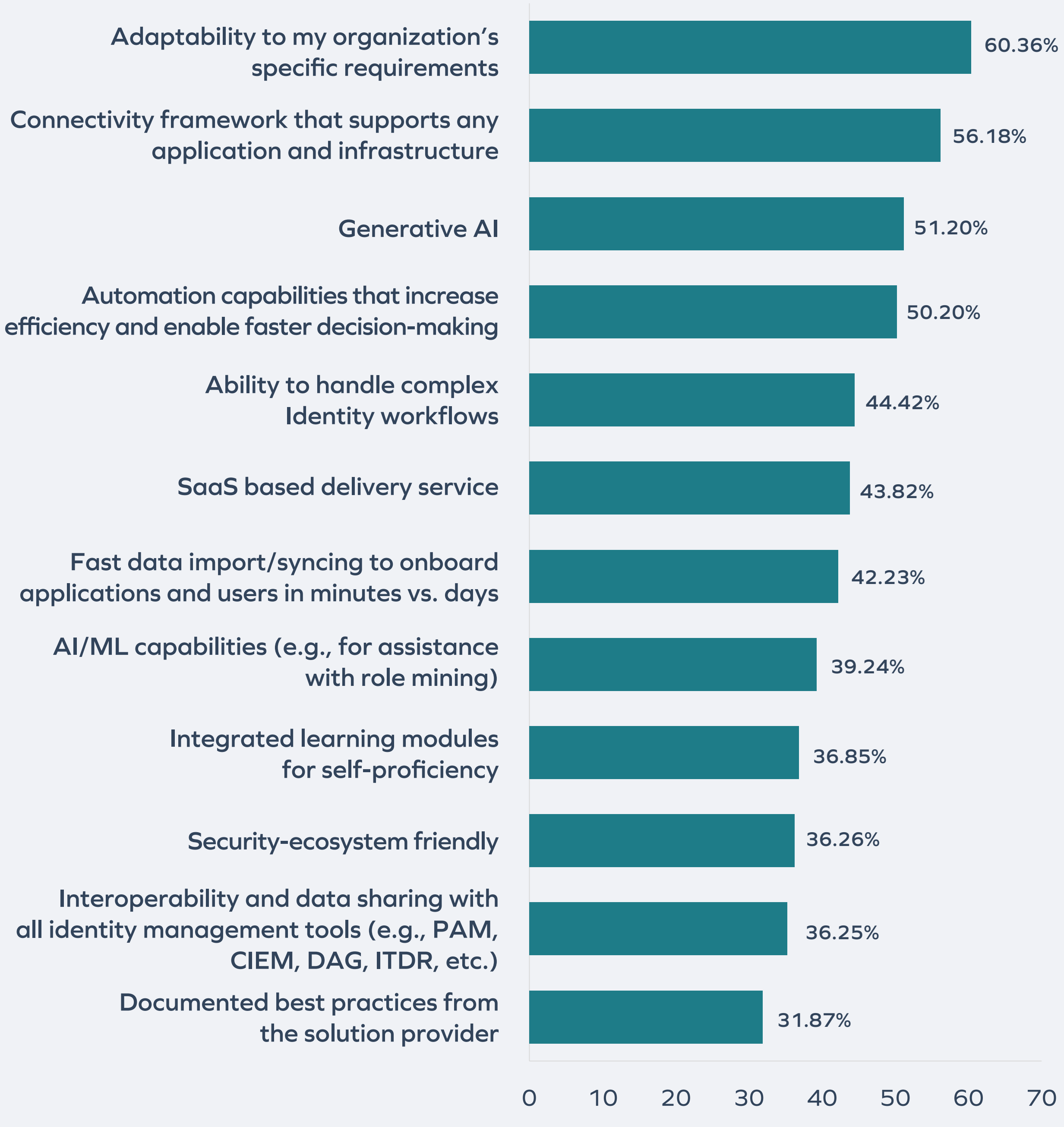


As more sensitive data and applications move to cloud-hosted environments, respondents assert that their organizations would get the greatest return on their investment by improving RBAC and visibility into cloud-based resources and well as behavioral activity functionality that could enabled them to better inform decisions and enhance policy definitions. Acquiring these specific features would certainly have a positive impact on bridging the performance deficiencies in the IGA solutions that many organizations currently use.

Evaluating new IGA solutions

Organizations are more frequently looking for adaptability, connectivity, automation, and generative AI features when evaluating new IGA solutions.

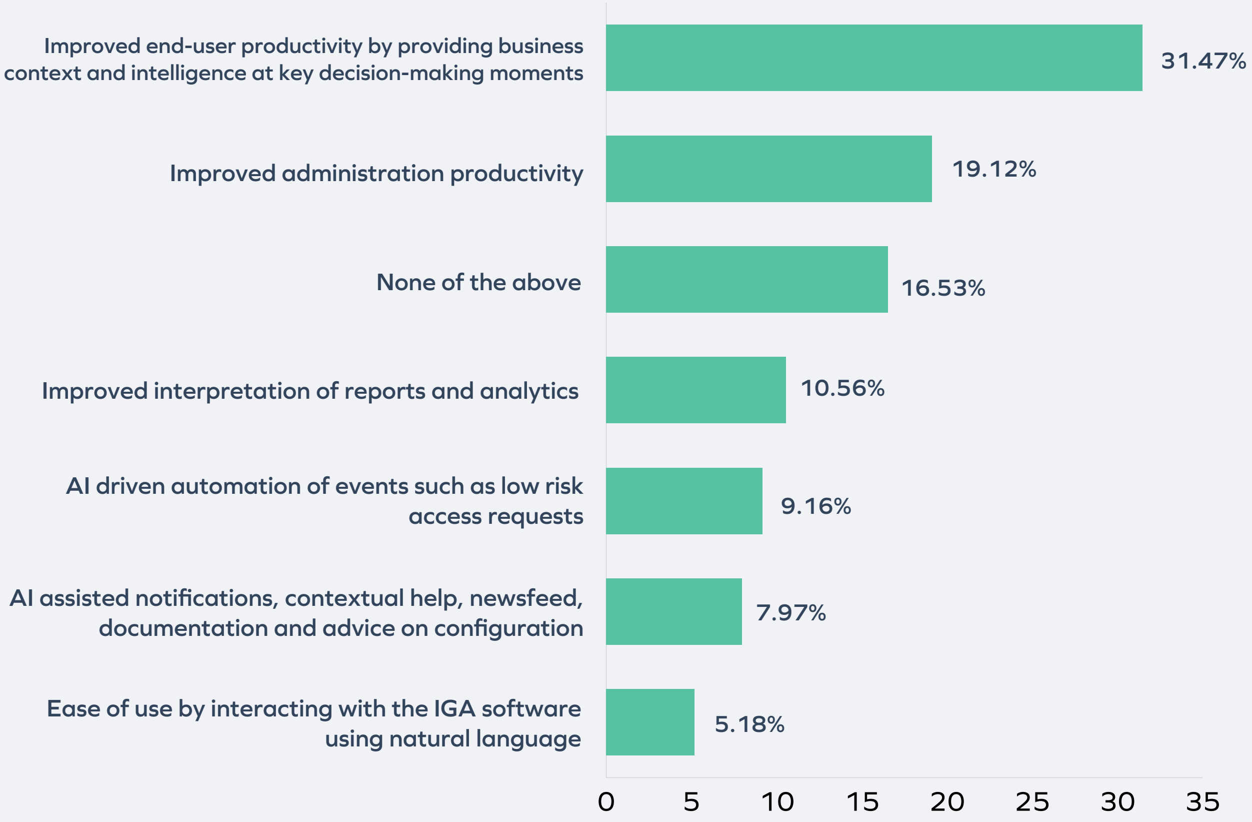
If your organization were evaluating a new IGA solution for deployment, which of the following characteristics would be most important?



To bridge existing functionality gaps, respondents said that a new IGA solution must be able to adapt to an organization's specific requirements (60.4%), automate core IGA policies (50.2%), and connect seamlessly with other applications and environments (56.2%). In addition, more than half of respondents (51.2%) report that Generative AI is critically important to them when evaluating a new IG solution.

Respondents report improving end-user productivity as the top outcome of using Gen AI assistants in an IGA solution.

Relating to the potential use of Gen AI assistants within IGA, which best describes the outcomes your organization would value:



When asked if having the ability to improve decision making by incorporating user behavioral activity to better inform decisions and enhance policy definition would be a top feature that would increase their organization's return on its IGA investment, 31.5% of respondents said it would. Respondents also assert that Gen AI assistants that could provide business context and intelligence at key decision-making moments, such as approvals and access reviews, could help improve end-user productivity and deliver high value in an IGA solution. Other Gen AI functions that respondents value include decreasing the time needed to onboard applications and configure policy that supports the principle of least privilege (19.1%) and improve report analytics (10.6%).

Conclusion: What these findings suggest about the State of IGA

IT security funding is better, but many organizations struggle with TCO. As business processes become more complex, most organizations using existing solutions are compelled to devote additional funding to time consuming upgrades and customization projects. A modern SaaS-based IGA solution adapts to an organization's specific needs and connects to external systems in cloud environments with no customization work required, keeping TCO low.

While a strong majority of organizations are confident in their core identity security competencies, overpermissioning and unnecessary access to sensitive resources continues to be a challenge. Organizations have historically focused on mitigating threats from external sources but the security professional's adage "most hackers don't break in, they log in" is still true. It is critical for identity security teams to have access control and identity governance processes to ensure users of their organizations' IT infrastructure have only the access they need to do their jobs and only for as long as they need it. This principle of least privilege is critical to mitigating threats such as compromised user credentials and misuse of privileged accounts,

Manual processes must be replaced with automation. The data strongly suggests that organizations are struggling with sustainable user lifecycle management. As organizations move more applications and sensitive data to cloud environments, managing user permissions across various systems manually will be even more cumbersome and customizing existing solutions to support automation of these processes will be less effective; making the implementation of a modern SaaS-based IGA solution an organizational imperative.

Cloud-based RBAC and user access visibility are high-impact features driving IGA return on investment. Improving operational efficiency of both access certifications and streamlined provisioning and gaining visibility into user access activity in cloud/multi-cloud/hybrid cloud infrastructure with a new SaaS-based IGA solution would pay immediate dividends for most organizations.

Generative AI is emerging as a top characteristic when evaluating a new IGA solution and organizations should be paying attention to the benefits it provides. Connectivity, adaptability, and automation remain top characteristics that organizations look for, but generative AI can provide business context and intelligence at key decision-making moments, such as approvals and access reviews is critical for improving end-user productivity. Generative AI can also improve administration productivity by cutting the time and effort required to onboard applications and configure policy that supports a Zero-Trust Security Model.

Recommended Actions

Address Security Gaps and Enhance IGA strategy

□ **Conduct a comprehensive audit of existing IGA capabilities** to identify inefficiencies, manual processes, and excessive permissions associated with user accounts.

□ **Establish clear policies for role-based (RBAC) and attribute-based access control** and implement multi-factor authentication (MFA) to strengthen access controls and improve security.

□ **Develop a roadmap to replace inefficient and time-consuming manual processes** and with automated workflows that enhance both security and operational efficiency.

Invest in a Cloud-based, AI-powered modern IGA solution

□ **Choose an IGA platform that provides modern SaaS capabilities** with built-in analytics that leverage Generative AI-powered insights for enhanced decision-making.

□ **Utilize vendor Generative AI capabilities** to streamline intelligence-driven access reviews using natural language interfaces via collaboration tools such as Zoom and Microsoft Teams.

□ **Ensure the solution offers robust scalability and uptime** to meet growing demands and maintain continuous access control.

□ **Verify that the IGA system aligns with evolving standards** to address regulatory compliance and evolving security threats.

Ensure regulatory compliance

□ **Regularly update and refine access policies to** reflect the evolving threat landscape and emerging risks, ensuring continuous alignment with best practices.

□ **Implement continuous monitoring and reporting mechanisms** to detect anomalous behavior and enable rapid incident response by notifying the appropriate authorities and security mitigation teams.

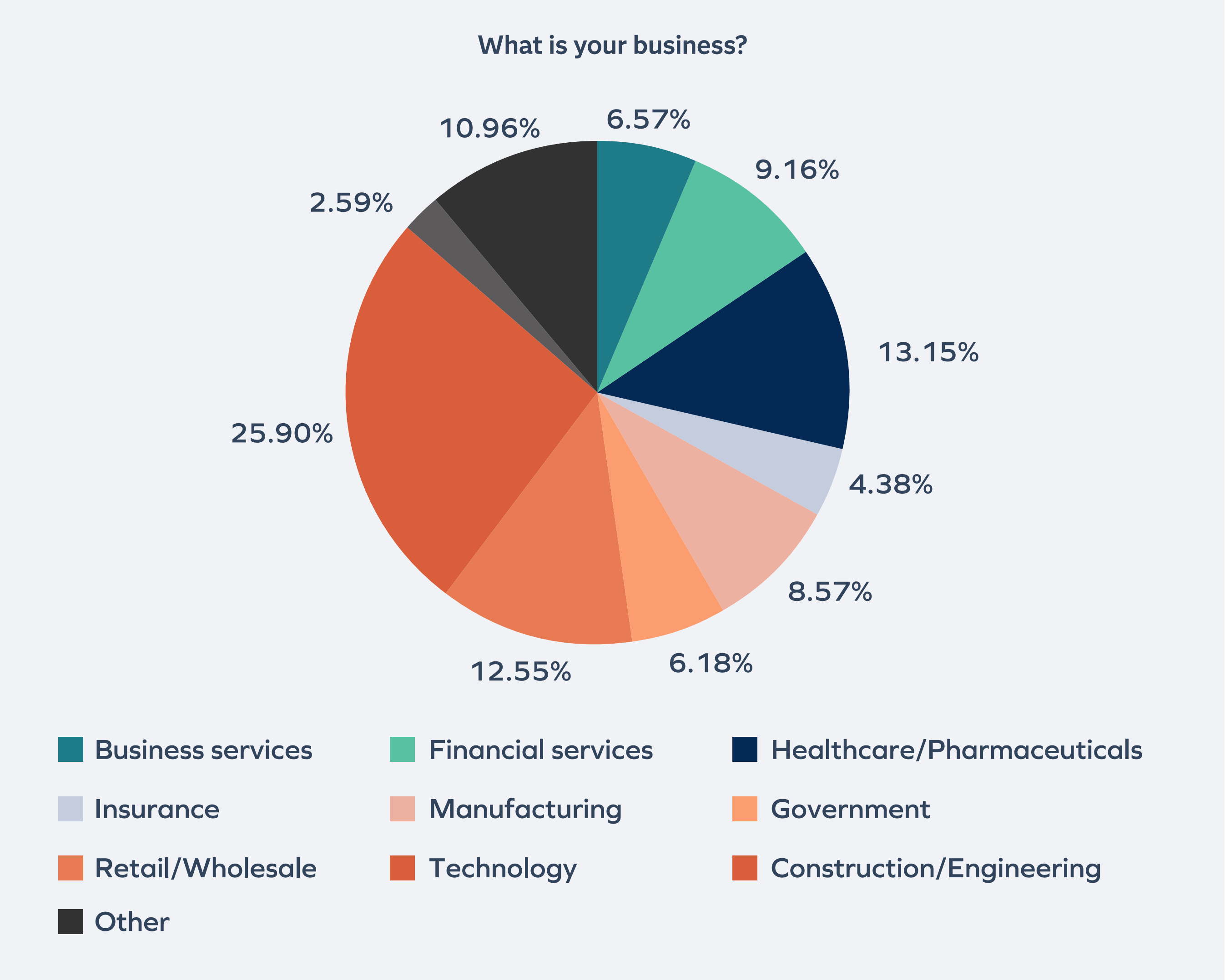
□ **Collaborate closely with compliance teams** to ensure that all IGA measures meet or exceed current legal and industry requirements to mitigate the risk of penalties and reputational harm.

Methodology

The research we conducted used a comprehensive survey of questions involving 502 enterprises across the United States with more than 1,000 employees, encompassing the perspectives of both IT and business leaders. The respondents consisted of people across a wide range of ages with about even gender breakdown (60-40, male to female) that are responsible for one of identity governance and access management, compliance, cybersecurity or general IT administration and management in organizations.

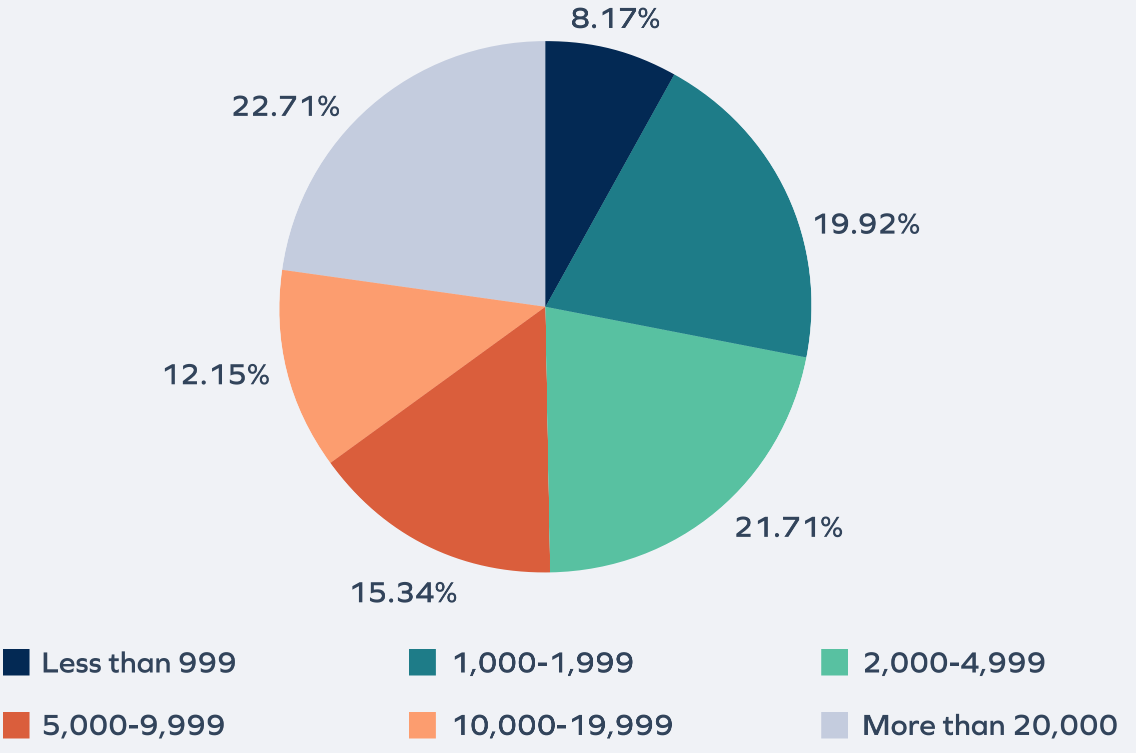
The organizations covered a wide spectrum of industries across every region of the United States.

Firmographic Data

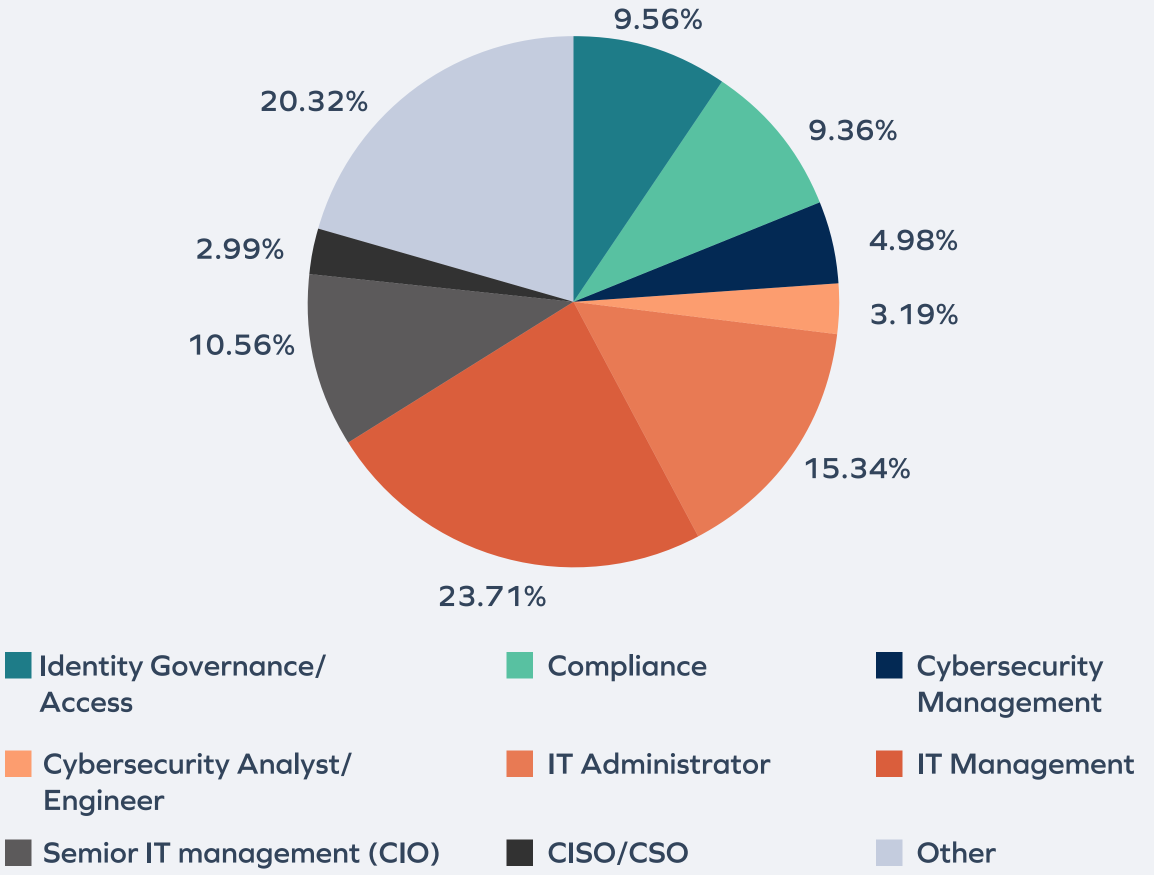


What is your business?

What is the size of your organization?



What is your role in your organization?



Omada

Omada simplifies Identity Governance by providing a full-featured, cloud-native IGA solution that streamlines the complex processes of managing user identities, access, and entitlements. With a focus on automation and user-centric design, Omada reduces manual tasks and enhances operational efficiency, ensuring that organizations can easily enforce security policies, comply with regulations, and manage user access at scale. By leveraging advanced technologies such as AI-driven decision-making and role-based access control (RBAC), Omada enables businesses to achieve stronger security, better compliance, and improved user experiences—without the complexities traditionally associated with identity governance.

V29012025