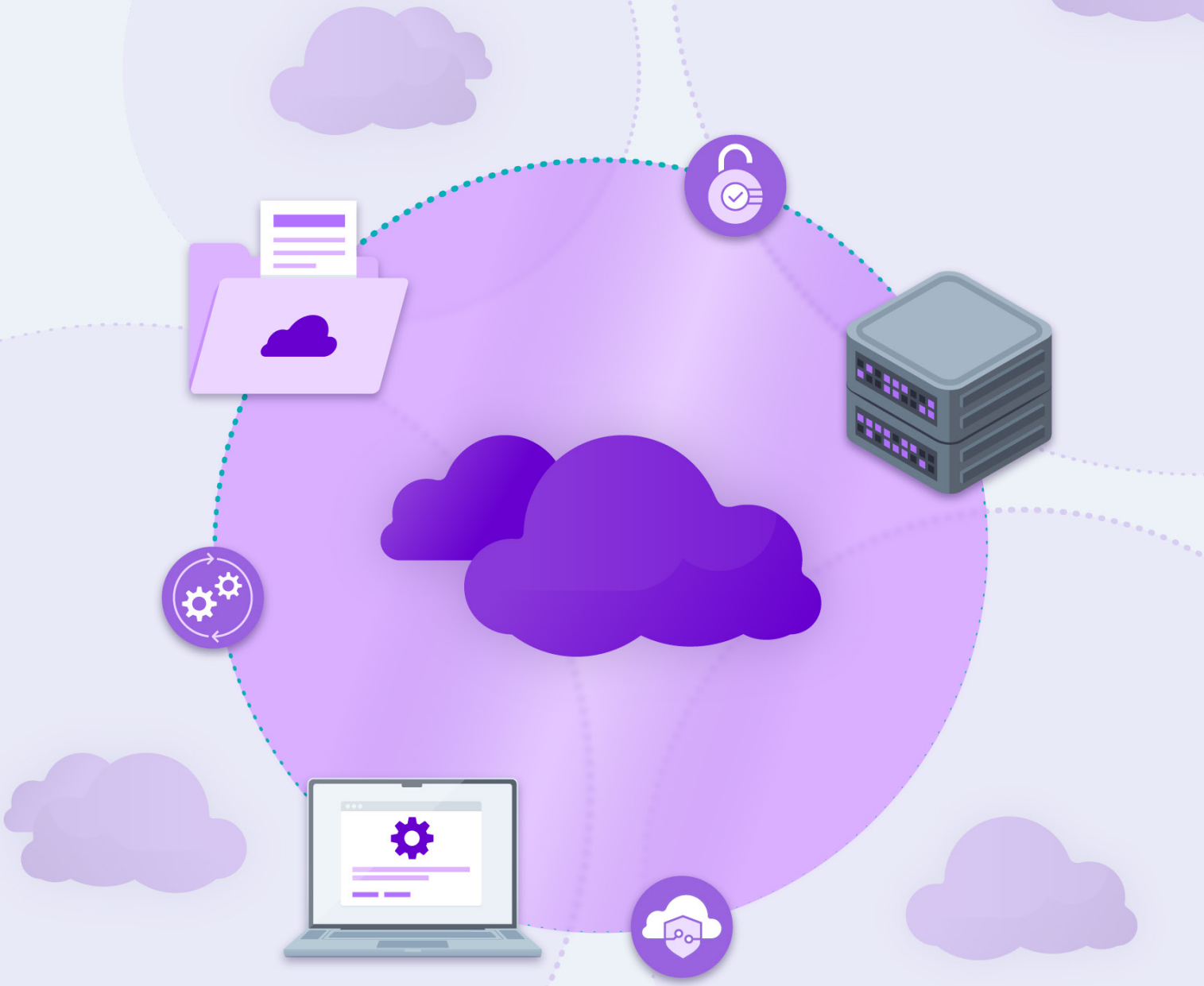
The State of Multi-Cloud Identity Survey

Insights and Trends for 2025



STRATA
Identity Orchestration

CSA cloud security alliance®

Acknowledgments

Lead Author

Hillary Baron

Contributors

Josh Buker
Marina Bregkou
Ryan Gifford
Sean Heide
Alex Kaluza
John Yeoh

Graphic Design

Claire Lehnert
Stephen Lumpe
Stephen Smith

Special Thanks

Heidi King and Michela Bellani

About the Sponsor

Strata is the Identity Orchestration leader, making consistent identity and policy management a reality. Their Identity Orchestration platform, Maverics, is the only solution built for today's distributed, multi-cloud and hybrid-cloud environments. With Strata, companies can quickly, securely, and permanently modernize applications to use cloud-based authentication and advanced identity solutions as well as enabling continuous identity availability.

https://www.strata.io/

Table of Contents

Acknowledgments 3
Key Findings 5
- Key Finding 1: The Double-Edged Sword of Multi-IDPs 6
- Key Finding 2: What Is Holding Back Progress with Modernizing Identity Systems? 7
- Key Finding 3: Visibility Gaps: The Achilles' Heel of Identity Management in Multi-Cloud Environments 9
- Key Finding 4: Investing in the Future: Strategic Identity Management Priorities 12
- Key Finding 5: The Hidden Weaknesses in Identity Resilience Strategies 13
- Key Finding 6: The Cost of Disruptions and Slow Recovery in Identity Services 15
  - Disruptions in Identity Services 15
  - The High Cost of Downtime 16
  - Bottom Line 17
- Conclusion 17
  - Strategic Priorities for Identity in 2025 17
  - A Path Forward: Be the Change Agent 19

Full Survey Results 20
- Identity Management Across Cloud Platforms 20
- Modernizing Identity 21
- Identity Continuity and Resilience 22
- Outages and Disruptions 25
- Identity Analytics 26
- Application Identity Governance 27
- Future of Directions and Investments 29

Demographics 30
Survey Creation and Methodology 31
- Goals of the Study 31

Key Findings

As enterprises accelerate their adoption of multi-cloud, they encounter significant obstacles in harmonizing hybrid and cloud identity systems for secure integration. These challenges include high costs related to Identity and Access Management (IAM) technical debt, a pronounced talent gap, vendor lock-in, and the complex task of rewriting legacy applications. Traditional tools no longer suffice; they struggle to keep up with the evolving complexities organizations deal with today.

To address unpredictability, it's critical to build a resilient identity infrastructure. Organizations seek deeper analytics and advanced governance tools to improve visibility across diverse identity providers (IDPs) in multi-cloud environments. This can introduce obstacles in business priorities and threaten the benefits of multi-cloud adoption.

Addressing these challenges is essential not only for security and compliance but also for operational efficiency and business agility. Organizations are expanding across diverse IDPs, so the need for deeper analytics, enhanced visibility, and advanced governance tools becomes increasingly critical. Although identity management complexity is growing, so are opportunities for innovation through solutions like identity fabric and orchestration. Identity fabric unifies identity systems across platforms and vendors, while identity orchestration automates and coordinates identity processes, address technical debt and strengthen identity management strategies by staying ahead of emerging threats.

This report highlights six key findings essential for overcoming the challenges of multi-cloud identity management:

1. The Double-Edged Sword of Multi-IDPs:
While multi-cloud/multi-IDP environments offer flexibility and enhanced security, it also adds complexity to managing access controls across disparate systems.

2. Barriers to Modernizing Identity Systems:
Decades of accumulated IAM technical debt, complexity, and resource constraints hinder organizations' efforts to modernize, slowing innovation and increasing risk.

3. Visibility Gaps in Multi-Cloud Environments:
The inability to manage all aspects of identity in fragmented cloud and hybrid environments creates serious security and compliance risks.

4. Strategic Investment in Identity Management:
Despite economic pressures, organizations recognize the need to invest in analytics, legacy system modernization, and IAM resilience to stay ahead of threats.

5. Hidden Weaknesses in IAM Resilience Strategies:
Many organizations find their efforts to build resilient identity infrastructures fall short, leaving them vulnerable to IDP-based outages and disruptions.

6. The High Cost of Identity Service Disruptions:
Slow recovery times and frequent disruptions aren't just operational issues—they have significant financial and reputational consequences.

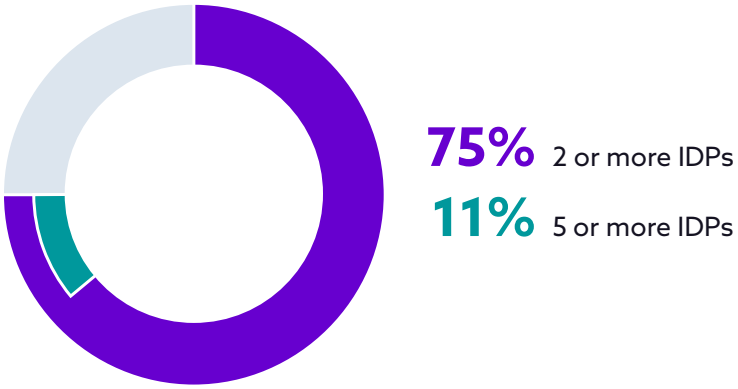
Organizations must address these challenges. This report diagnoses the current landscape and provides a roadmap for change. By leveraging the insights and recommendations, you can strengthen processes, upgrade technology, and adopt new solutions to make meaningful progress to help you create a resilient identity management plan that supports your organization's future growth.

Key Finding 1:

The Double-Edged Sword of Multi-IDPs

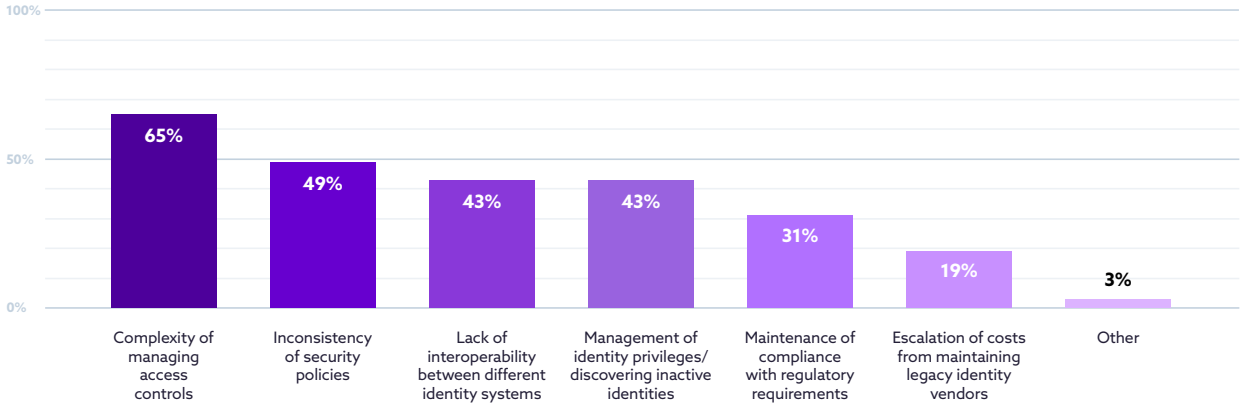
As we approach 2025, multi-cloud identity management has reached a critical juncture for IAM teams. The majority **(75%) of organizations now manage two or more IDPs**, with **11% relying on five or more**. This multi-IDP approach is especially **prevalent in enterprises with annual revenues exceeding $1 billion, where 40% use more than three IDPs**. This trend is driven both by the desire for best-in-class services and the need for identity services specific to their infrastructure. But it also introduces complexity and underscores the need for robust identity strategies capable of securing and managing these environments effectively.

Number of IDPs organizations use across all environments.



Organizations adopting multiple IDPs tend to show higher maturity levels in IAM resilience and greater confidence in their identity management programs. However, this presents significant challenges. Chief among these challenges is the **complexity of managing access controls across disparate systems**, a concern cited by 65% of respondents. This is consistent with the top challenge from the previous year's State of Multi-cloud Identity Report 2023, as organizations wrestle with managing fragmented applications and user identities across multiple cloud platforms. This indicates organizations have not found a sufficient strategy for addressing this issue. Other top challenges include 49% of organizations struggling with the inconsistency of security policies, 43% report difficulties due to the lack of interoperability between identity systems, and another 43% identified management of identity privileges or discovering inactive identities.

Biggest challenges with identity management across multiple cloud platforms.



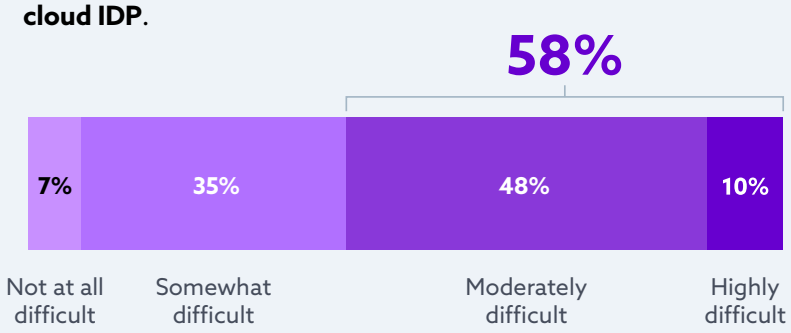
Multi-IDPs introduce complexity, highlighting the urgent need for robust, interoperable identity solutions. However, as organizations expand multi-cloud architectures, they face the challenge of modernization, so the infrastructures managing risk don't become bottlenecks that stifle innovation and growth. However, modernizing identity systems is no small feat; it presents a set of challenges for organizations to navigate carefully to ensure they are fully prepared for the demands of the future.

Key Finding 2:

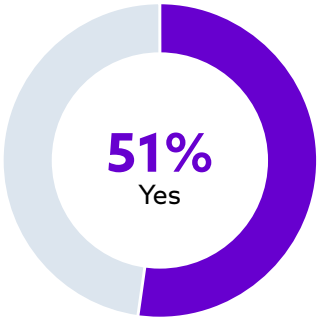
What Is Holding Back Progress with Modernizing Identity Systems?

As enterprises modernize their identity systems to keep pace with multi-cloud strategies, they find themselves in a quagmire of technical debt, complexity, and resource constraints. While **51%** of organizations have embarked on, or are planning to, undertake identity modernization efforts, the road to success has significant obstacles that can impede progress and stymie innovation.

More than half **(58%) of organizations report moderate to high difficulty when it comes to onboarding on-premises apps to a cloud IDP**.



Have or plan to migrate application identity from on-premises to cloud with cloud IDP vendor.



At the heart of the difficulty organizations are encountering is the burden of multi-generational legacy systems. Over half of the organizations (54%) cite technical debt as their top hurdle when modernizing their IAM architecture, with 45% grappling with the risks associated with data migration and integrity. The struggle is exacerbated by difficulties in securing stakeholder buy-in, a challenge noted by 41% of respondents. This trifecta of obstacles—technical debt, data risks, and stakeholder resistance—creates barriers to modernization efforts.

Top challenges organizations face in modernizing IAM architecture.

54% Tech debt from legacy identity systems

45% Data migration and integrity risks

41% Stakeholder buy-in/ conflicting priorities

36% Lack of available expertise

33% Length of time to rewrite applications

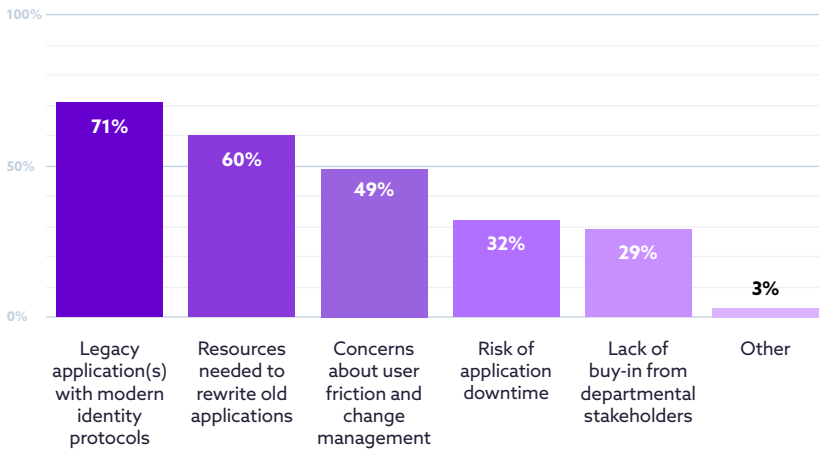
32% Vendor lock-in

28% Lack of budget for services

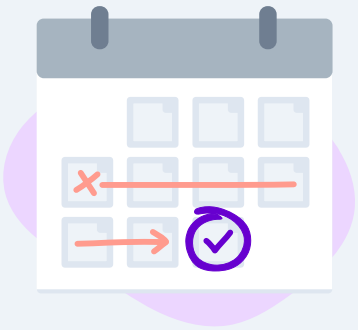
The impact of these challenges is felt across all levels of the organization, but particularly among staff-level employees who deal with the day-to-day realities of managing outdated systems. A notable 55% of staff members identify technical debt as their primary challenge, while 48% point to a lack of expertise. This awareness among the "boots on the ground" highlights the strain placed on those tasked with implementing new solutions while maintaining legacy systems.

When asked about what barriers organizations experience when deploying advanced authentication for their applications, several key issues were identified. **The most common response was incompatibility with non-standard, legacy applications (71%), further highlighting the issue of tech debt**. Another 60% reported lacking the resources for rewriting applications, and another 49% identified concerns about user friction.

Barriers to deploying advanced authentication for all applications.



62% of organizations have had to postpone essential projects due to the lack of available identity talent



While hiring additional talent may help resolve some of these issues, it's not without its own difficulties and drawbacks. The 2023 State of Multi-cloud Identity Report found that over half of the organizations (52%) reported that finding talent with the necessary experience to modernize applications off legacy systems is "difficult" or "very difficult." In other words, organizations will struggle to hire their way out of these challenges. It was also found that **62% of organizations have had to postpone essential projects due to the lack of available identity talent**, further delaying progress and hindering their ability to address tomorrow's IAM challenges. This delay not only affects modernization efforts but also undermines the organization's strategic initiatives and its ability to stay competitive.

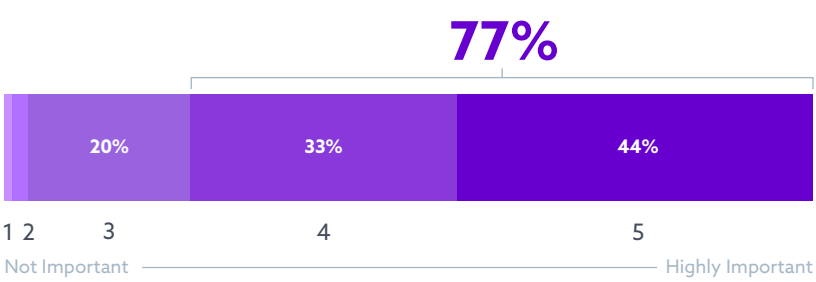
A better strategy is for organizations to prioritize investing in tools and technologies (e.g., identity orchestration) to help automate many of these manual processes within identity management, reducing the burden on security and technology teams. By doing so, businesses can maximize the efficiency of the talent they already have, enabling them to do more with less. This approach fosters a proactive mindset, allowing organizations to focus on preventing future issues rather than getting bogged down in mitigating immediate concerns, which only perpetuates the cycle of technical debt.

Key Finding 3:

Visibility Gaps: The Achilles' Heel of Identity Management in Multi-Cloud Environments

The importance of visibility into organizations' identity management cannot be overstated, particularly with the increasing complexity of their cloud environments. The adage "*you can't secure what you can't see*" holds particularly true in this context. Despite the critical role of visibility in ensuring robust security and compliance, many organizations find themselves struggling with significant gaps in their tooling, leading to a lack of comprehensive oversight across their multi-cloud environments.

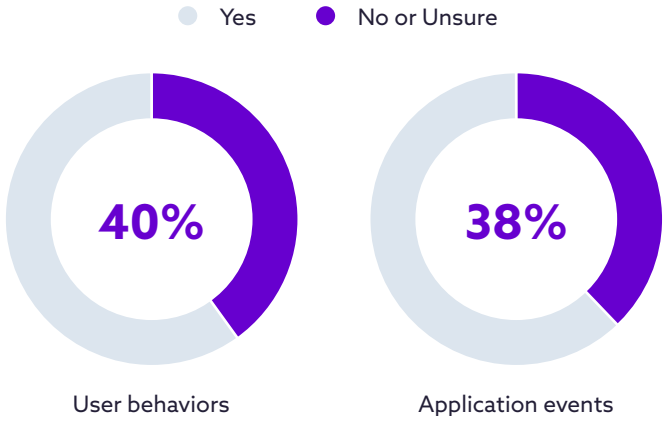
Importance of analytics that provide visibility into organization's IAM environments.



The data clearly shows that organizations place a high value on visibility within their IAM environments. In fact, **77% of respondents rated visibility as highly important**, many recognized that effective risk management and compliance efforts depended on it. However, there is a significant disconnect between the importance placed on visibility and the reality of what organizations are actually achieving.

Unfortunately, the reality on the ground reveals substantial visibility gaps that hinder effective identity management. Over one-third of organizations express dissatisfaction or uncertainty regarding their ability to monitor and control several key areas within their IAM environments.

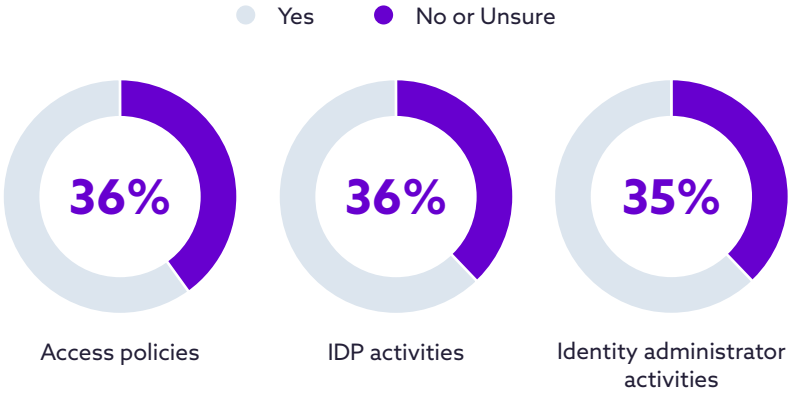
Does your organization have visibility into the follow items?



For instance, 40% of organizations report inadequate visibility into user behaviors, which limits their ability to understand and report on how users interact within their systems. Similarly, 38% of respondents struggle to maintain visibility into application events, making it difficult to track and respond to critical incidents as they unfold. This is because disparate traditional identity services exist in silos and do not interoperate well.

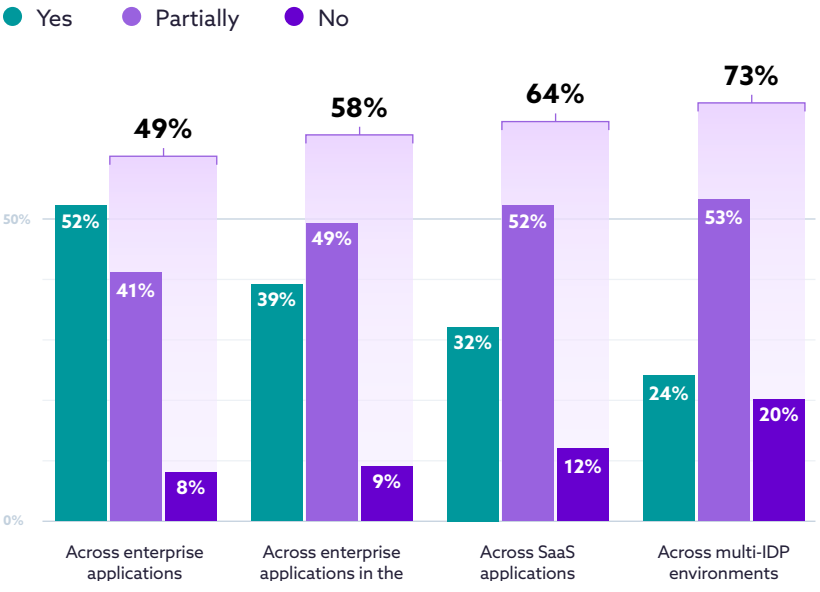
Access policies, another crucial component of IAM, are also affected by visibility issues. **About 36% of organizations report challenges in overseeing how these policies are applied and enforced, which can lead to inconsistencies and potential security risks**. This issue extends to monitoring the activities of IDPs, where another 36% of respondents express concerns over their lack of insight. This problem is compounded by 35% of organizations reporting insufficient visibility into identity administrators' actions.

Does your organization have visibility into the follow items?



These visibility gaps are likely exacerbated by the shortcomings of their current tools and types of applications. When organizations were asked about the effectiveness of their Identity Governance and Administration (IGA) tools, many indicated that these tools need to meet their needs across several critical areas. Specifically, **73% of respondents reported that their IGA tools fall short in managing identities across multiple IDPs**, a concerning statistic given the widespread use of multiple IDPs within organizations.

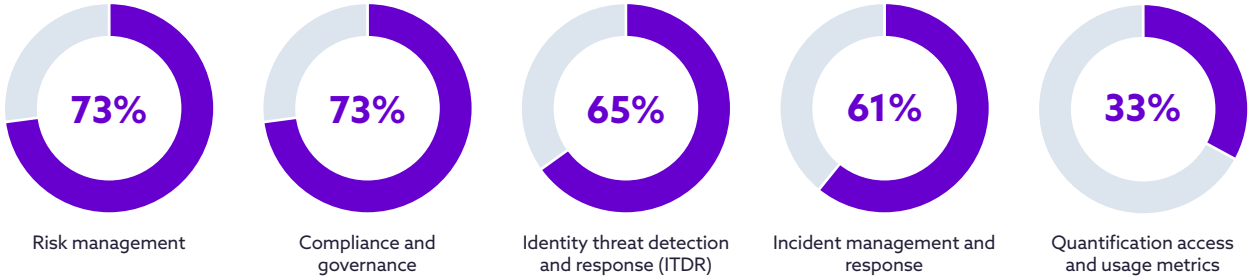
Are Identity Governance tools meeting organizations' needs in these areas?



Furthermore, **64% of organizations found their tools inadequate for managing identities within SaaS applications**. This is another important factor given that organizations' use of SaaS increases with each year. Another 58% experienced similar challenges with cloud-based enterprise applications. Even **within on-premises environments, 49% of respondents indicated that their tools were not fully meeting their needs**. This highlights the difficulties faced in hybrid environments where both cloud and on-premises systems must be managed simultaneously.

The lack of adequate visibility tools is not just an operational inconvenience; it has serious implications for risk management, compliance, and incident response. The data reveals that **73% of organizations believe that improved visibility is essential for enhancing their risk management capabilities**. Similarly, another 73% stress the importance of visibility in maintaining compliance and governance, particularly as regulations, such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Digital Operational Resilience Act (DORA) become more stringent and complex.

Reasons organizations require better visibility.



Moreover, improved visibility is seen as crucial for bolstering Identity Threat Detection and Response (ITDR) efforts, with **65% of respondents indicating that better visibility would significantly strengthen their ability to detect and respond to identity-based threats**. In addition, 61% of organizations recognize the need for enhanced visibility to improve their incident management and response strategies, ensuring they can quickly and effectively address security incidents when they occur.

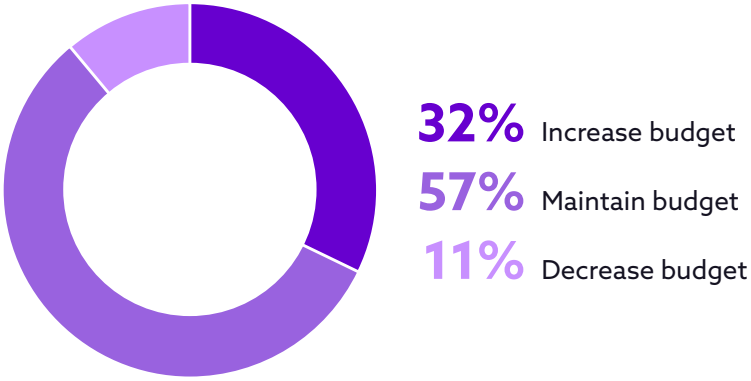
The data makes it clear that while organizations understand the critical importance of visibility in securing their multi-cloud environments, their current tools and strategies are insufficient. As the complexity of multi-cloud architectures grows, so too does the need for comprehensive, integrated visibility solutions that can bridge these gaps efficiently. Without addressing these visibility challenges, organizations will continue to face significant risks, not only in terms of security breaches but also in meeting compliance requirements and effectively managing incidents.

Key Finding 4:

Investing in the Future: Strategic Identity Management Priorities

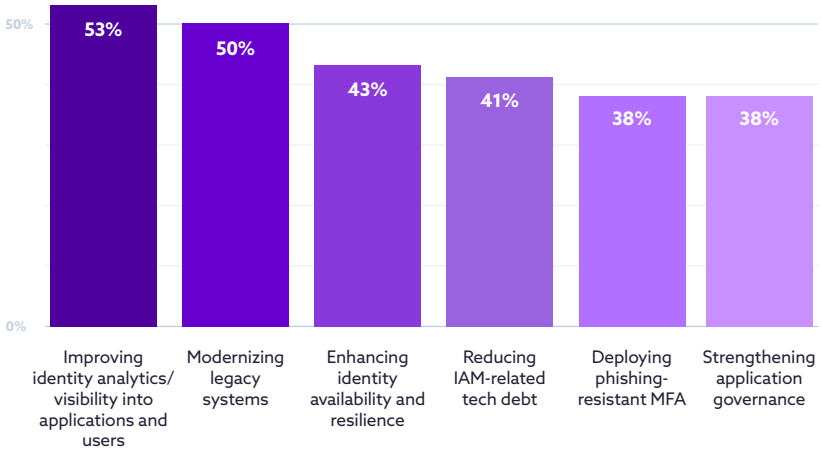
As organizations navigate the complexities of multi-cloud environments, the importance of robust identity management has never been clearer. Despite economic pressures, only 11% of organizations are considering reducing their identity management budgets, highlighting the critical need to address ongoing challenges. Most organizations are maintaining or increasing investments, focusing on areas that align closely with the pain points identified in previous key findings.

Anticipated budget changes for identity management solutions in the next 12 months.



Looking ahead to 2025, organizations are prioritizing investments in key areas that directly address the challenges highlighted in earlier findings. **Improving identity analytics and visibility is a top priority for 53% of organizations**, reflecting the visibility gaps discussed in Key Finding 3, where inadequate tools hinder effective risk management and compliance. Additionally, 50% are focused on modernizing legacy systems, a response to the technical debt and outdated infrastructures highlighted in Key Finding 2.

Prioritized areas of identity and access management for future investment.



Enhancing identity availability and resilience (43%) and reducing IAM technical debt (41%) are also critical priorities. This addresses the need for continuous improvement in identity management capabilities as organizations contend with the complexities of multi-IDPs outlined in Key Finding 1.

It's clear that organizations are not only aware of the challenges they face in managing identity in a multi-cloud world but are also concerned enough to be taking concrete steps to try to address them. By aligning their investments with the specific pain points they have identified, they are **setting the stage for more secure,**

resilient, and agile identity management systems by 2025. As IAM teams increasingly take on a more prominent role in supporting overall business initiatives, their decisions in building secure, resilient, and agile identity management systems by 2025 are becoming key competitive differentiators. This forward-thinking approach is essential for staying ahead of the evolving threats and ensuring that their identity infrastructures are orchestrated and can support the demands of the future.

Key Finding 5:

The Hidden Weaknesses in Identity Resilience Strategies

As organizations strive to build resilient identity infrastructures capable of withstanding the ever-present threats of service outages, network disruptions, and cyberattacks, many are discovering that their efforts are falling short. Despite deploying a range of strategies to ensure IAM resilience, the majority of organizations remain unprepared for the full spectrum of identity-related challenges.

Preventative measures organizations employ to ensure continuous availability of identity services.

69% Disaster recovery planning

66% Automated failover to secondary systems

65% High availability configurations

63% Real-time threat detection and mitigation

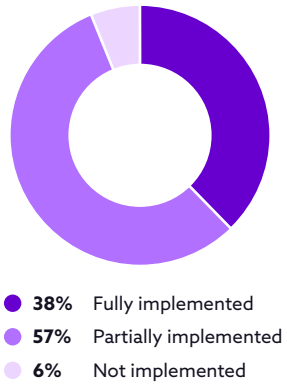
63% Regular system updates and patch management

51% Geo-redundancy

32% Redundant authentication methods

Organizations are not ignoring the importance of identity resilience. The data shows that **69% of organizations are engaged in disaster recovery planning, 66% have implemented automated failover systems, and 65% have configured their systems for high availability**. Additionally, 63% utilize real-time threat detection and mitigation, while another 63% commit to regular system updates and patch management. These measures are critical steps toward creating a robust identity management infrastructure capable of continuous operation. However, it's important to point out the potential misinterpretation of these options as referring to other IT systems, especially with the option of automated failover to secondary networking or computing platforms. This misinterpretation seems more likely for at least some respondents when the extent of implementation is taken into account.

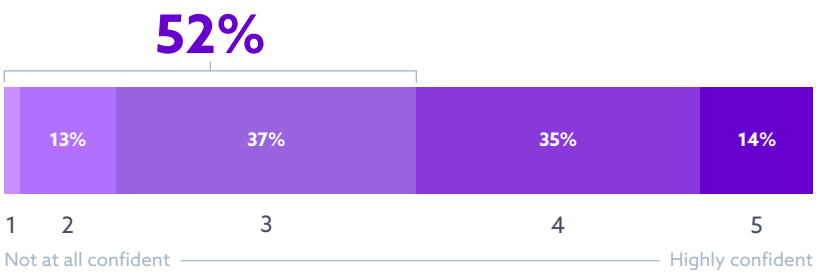
Status of Solution Implementation for Continuous Availability of Identity Services



Most organizations have not fully implemented these measures, and confidence in their identity infrastructures remains low. Only **38% of organizations report having fully implemented measures to ensure continuous availability of identity services**, while a troubling 6% admit to having nothing in place at all.

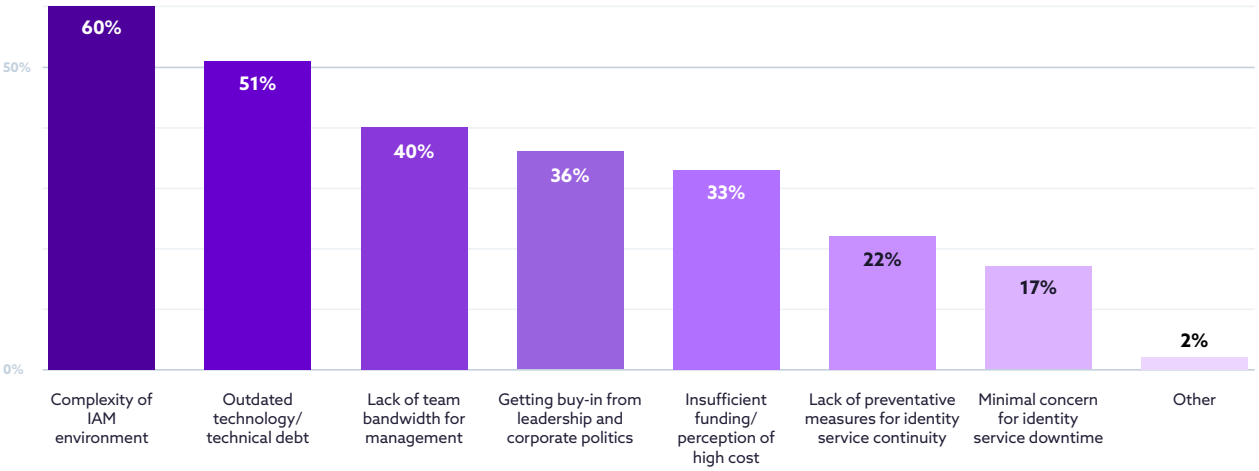
Furthermore, **52% of respondents feel only moderately confident—or worse—in their ability to withstand and recover from identity outages or disruptions**.

Confidence in organization's IAM infrastructure ability to withstand and recover from identity outages, disruptions, or attacks.



The challenges organizations face in achieving true identity resilience are multifaceted, rooted in the complexity of their IAM environments, outdated technology, and a lack of resources. **A significant 60% of respondents cite the complexity of their IAM environments as a major hurdle, while 51% struggle with the burden of outdated technology and technical debt.** Compounding these issues is a lack of bandwidth for effective management, with 40% of organizations acknowledging that they simply don't have the resources to maintain and enhance their identity infrastructures. **This shortage of resources forces organizations into a reactive security posture—focused on fixing immediate issues but unable to address future threats.** As a result, they are prevented from adopting a more proactive and innovative approach to security, one that would enable them to pursue cutting-edge projects and better prepare for emerging challenges.

Barriers to achieving a resilient identity infrastructure.



The pursuit of a resilient identity infrastructure is a critical objective for organizations operating in a multi-cloud world, but the gap between intention and implementation remains wide. While many are taking significant steps toward resilience, the majority still lack confidence in their identity infrastructure and do not have fully implemented systems necessary to withstand the challenges ahead. Addressing the underlying issues of **complexity, outdated technology, and resource constraints is essential if organizations are to build truly resilient identity infrastructures that can weather the storms of tomorrow**.

Key Finding 6:

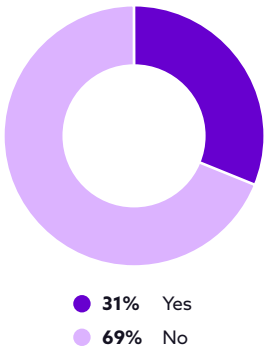
The Cost of Disruptions and Slow Recovery in Identity Services

Organizations recognize the critical importance of preventing downtime and ensuring rapid recovery to maintain operational continuity. However, despite their efforts, many struggle to meet the demands of their business environments, with significant impacts on risk, revenue, compliance, and reputation.

Disruptions in Identity Services

Organizations are aware of the **dual necessity of both preventing downtime and having robust recovery plans in place**. A significant 68% of respondents consider these two aspects equally important. Yet, even with prevention as a priority for 24% of organizations, many still fall short of the measures needed to support their business adequately. **Disruptions are not a rare occurrence**; 31% of organizations reported experiencing at least one disruption. Alarmingly, among those who experienced disruptions, nearly half **(48%) reported more than one incident**, with organizations possessing immature identity resilience programs being particularly vulnerable (53% compared to 41% in mature organizations).

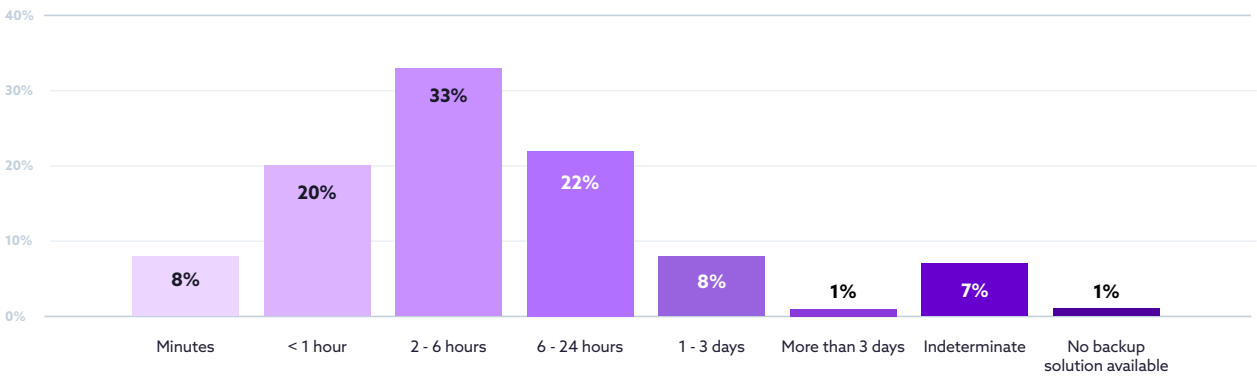
Business operations disrupted by cloud identity service downtime.



Recovering from a Disruption

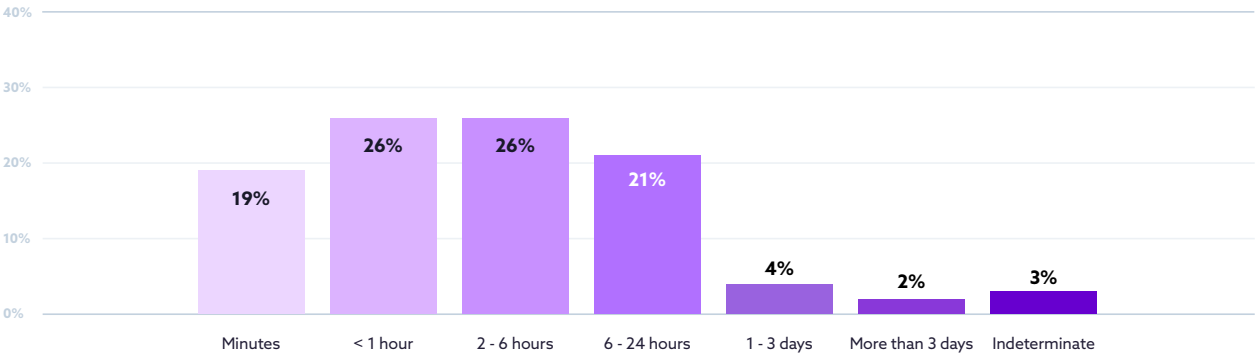
Timelines for recovering from identity service disruptions are another area where many organizations find themselves inadequately prepared. **Only 28% of respondents indicated that they could implement recovery measures within the hour**, a stark contrast to the 45% of organizations that need to recover within an hour to avoid unaffordable impacts to the organization. The need for rapid recovery is clear, with most organizations aiming to recover within minutes or hours to minimize operational disruptions.

Timeline to recover from a disruption.



Organizations with more mature identity resilience programs are more likely to report faster recovery times; 39% can recover within an hour, compared to only 17% among those with less mature programs. However, even these more prepared organizations recognize the need for improvement, as 51% report that the maximum downtime they can tolerate is under an hour. The importance of maturing identity resilience programs can not be overstated, as the ability to recover quickly is crucial for minimizing the impact of disruptions.

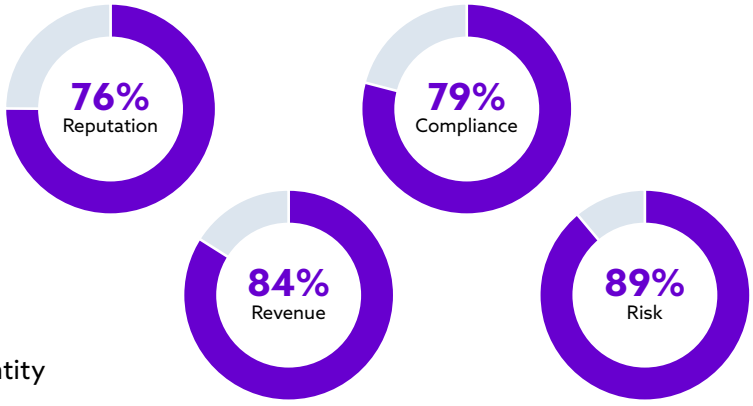
Maximum downtime organizations can afford for identity service disruptions.



The High Cost of Downtime

The impacts of downtime extend far beyond mere inconvenience, affecting every aspect of business operations. Drawing from the 2023 State of Multi-Cloud Identity report, we see that most organizations experience multiple outages each year, with regulatory fines, decreased revenue, and customer attrition being some of the most frequently reported costs. According to The Hidden Costs of Downtime report, **the average Global 2000 company loses $200 million annually due to unplanned downtime, with every minute of downtime costing an average of $9,000** – amounting to over half a million per hour. These figures underscore the high stakes involved and the pressing need for robust identity resilience.

Title areas of the organization impacted by an outage.



Further compounding the issue, downtime's hidden costs can be just as damaging as the direct ones. These include diminished shareholder value, lost customers, and a tarnished reputation, all of which can take months or even years to recover from (if they ever do). The financial repercussions of downtime should serve as a wake-up call for organizations to invest more heavily in their identity resilience programs, as the costs of inaction are simply too high.

Bottom Line

In an era where business continuity and survivability are paramount, the ability to prevent downtime and recover swiftly from identity service disruptions is not just a technical necessity but a business imperative. Organizations must recognize that disruption will happen (not 'if' but 'when') and that the costs of inadequate identity resilience are mounting. By prioritizing investments in both prevention and rapid recovery, businesses can better protect themselves against the inevitable identity service disruptions. To achieve this, organizations should explore flexible and resilient identity solutions, such as composable identity fabric architectures, which can help ensure that continuous app access is no longer an aspirational goal but a practical reality.

Conclusion

The findings in this report paint a clear picture: while organizations are making strides in managing identity in multi-cloud environments, significant gaps remain, particularly in resilience, visibility, interoperability, and recovery capabilities. However, the challenges outlined should not lead to a sense of despair. Instead, they provide an actionable guide for improvements that can greatly enhance both security and operational efficiency.

Strategic Priorities for Identity in 2025

This report has highlighted several key areas where organizations must focus their efforts to strengthen identity management.

1. Close the Visibility Gaps for Comprehensive IAM Insights

The inability to see and manage all aspects of identity across complex cloud environments is a major struggle, leading to serious security and compliance risks. To address this, organizations must ensure they have the right tools, architecture, and processes in place to gain complete visibility into their identity and access management (IAM) environments. This means investing in solutions to build an identity fabric and orchestrate that provide real-time insights into user behaviors, application events, and consistent access policies across all platforms. By enhancing visibility, organizations can not only improve security but also streamline compliance efforts and reduce the likelihood of costly disruptions.

2. Break Free from Identity Technical Debt by Modernizing and Automating IAM

Technical debt, system complexity, outdated solutions, and resource constraints are hindering organizations' best-intentioned efforts to modernize their identity and IT infrastructures, slowing innovation and increasing risk. Organizations should prioritize the modernization of legacy systems and automate as many IAM processes as possible. Modernizing IAM (e.g., using identity

orchestration) can streamline the management of disparate identity systems, facilitate the integration of new technologies, and automate key processes. This transformation will not only free up valuable resources and reduce human error but will also drive innovation, improve agility, and enhance security measures—empowering organizations to stay ahead of emerging threats and capitalize on new opportunities.

3. Build a Resilient Future by Strengthening Identity Infrastructure

Many organizations are discovering that their efforts to build resilient identity infrastructures fall short, leaving them vulnerable to outages and disruptions. Building a resilient identity infrastructure is not a one-time effort but an ongoing commitment that may require a fundamental re-architecting of current systems. Using an identity fabric with orchestration can play a crucial role in this process by ensuring that redundant identity services are distributed and resilient across multiple environments. Additionally, incorporating tools that offer IDP health checks and simulated downtime exercises can further strengthen resilience by proactively identifying weaknesses and preparing for future disruptions. Organizations should focus on developing both preventative measures and robust recovery plans, regularly testing and updating these plans to maintain a strong defensive posture.

4. Simplifying Complexity: Proactively Manage Multi-IDPs

While multi-IDPs offer flexibility and enhanced security, they also introduce significant complexity in managing access controls across disparate systems. To turn these challenges into opportunities, organizations should adopt a proactive approach to identity management, addressing current issues while anticipating future threats and vulnerabilities. Identity orchestration can be a game-changer, simplifying the management of multiple IDPs, ensuring seamless integration, and reducing the complexity of access control across various systems.

By shifting from a reactive to a proactive security posture, IAM teams have the chance to elevate their role within the organization. Rather than being seen solely as a cost center, IAM can become a strategic partner that supports the CEO's mission and vision. By solving critical challenges and enhancing identity management, IAM teams can contribute to competitive differentiation and innovation, helping the business achieve its goals. In doing so, IAM not only safeguards operations and mitigates risks but also drives business success and supports overall business strategies, not just IT ones.

5. Ensure Identity Resilience with Failover Strategies

Identity resilience is a critical component of resilience, particularly in a multi-cloud world where outages—planned or unplanned—can disrupt business operations. To mitigate the impact of identity service disruptions, organizations must implement robust failover strategies that automatically switch to secondary IDPs when needed. Leveraging software that supports seamless failover to a secondary IDP during planned maintenance or unplanned outages will help ensure that identity services remain "always on." This continuity strategy not only strengthens security but also enhances operational efficiency, allowing businesses to maintain continuous access and prevent downtime from negatively impacting the user experience.

6. Strategic Identity Investments for 2025 and Beyond

Despite economic pressures, organizations recognize the need to invest in key areas like analytics, legacy system modernization, and identity resilience to stay ahead of threats. An identity fabric used through orchestration provides the strategic advantage needed to integrate and manage multiple identity systems seamlessly. By investing in these solutions, organizations can ensure that their IAM strategies not only address immediate security concerns but also align with broader business goals. This investment will help organizations stay competitive, differentiate themselves in the market, and drive innovation.

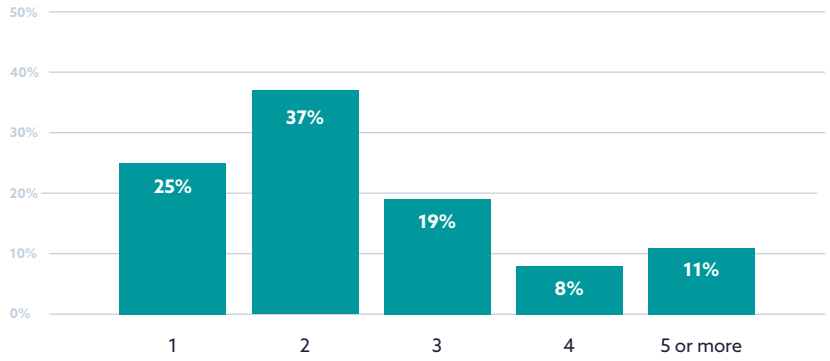
A Path Forward: Be the Change Agent

The path forward is clear; organizations that recognize and act on the insights from this report will be better equipped to navigate the complexities of multi-cloud identity management. By taking decisive, practical actions today—such as embracing identity orchestration technologies—IAM teams can move beyond their traditional roles, becoming key enablers of innovation, driving competitive advantage, and contributing directly to business growth.

Full Survey Results

Identity Management Across Cloud Platforms

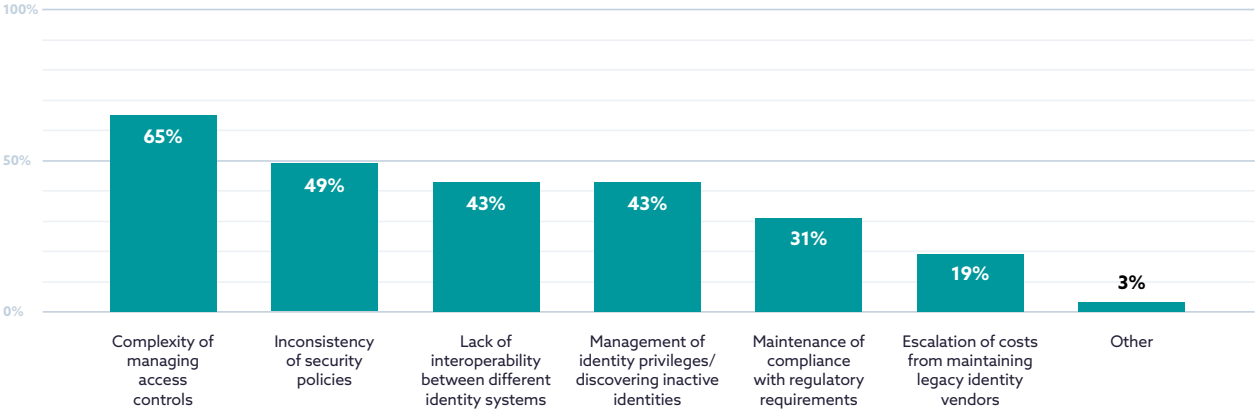
Number of IDPs organizations use across all environments.



Types of identity services organizations currently use.

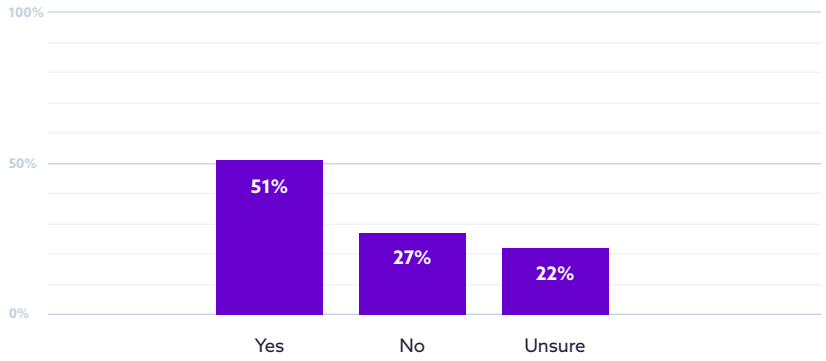
97%	Multi-Factor Authentication (MFA)	**32%**	Identity Threat Detection and Response (ITDR)	**19%**	Know Your Customer (KYC)
81%	Privileged Access Management (PAM)	**21%**	Risk Signals	**5%**	Attribute Stores
51%	Cloud Access Security Broker (CASB)	**20%**	Fine-grained Authorization Service	**2%**	Other (specification required)
36%	Identity Governance and Administration (IGA)	**19%**	Identity Proofing		

Biggest challenges with identity management across multiple cloud platforms.

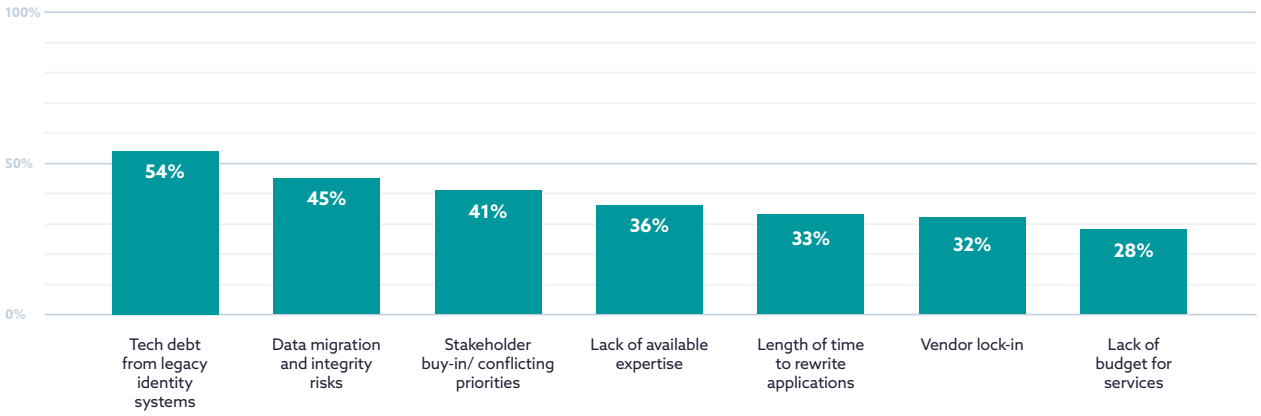


Modernizing Identity

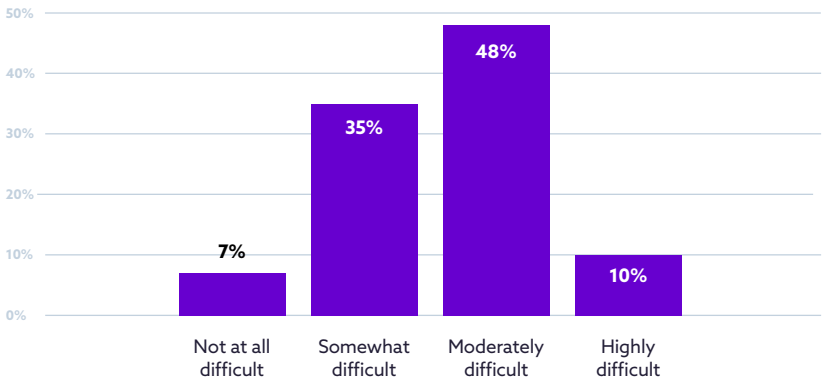
Have or plan to migrate application identity from on-premises to cloud with cloud IDP vendor.



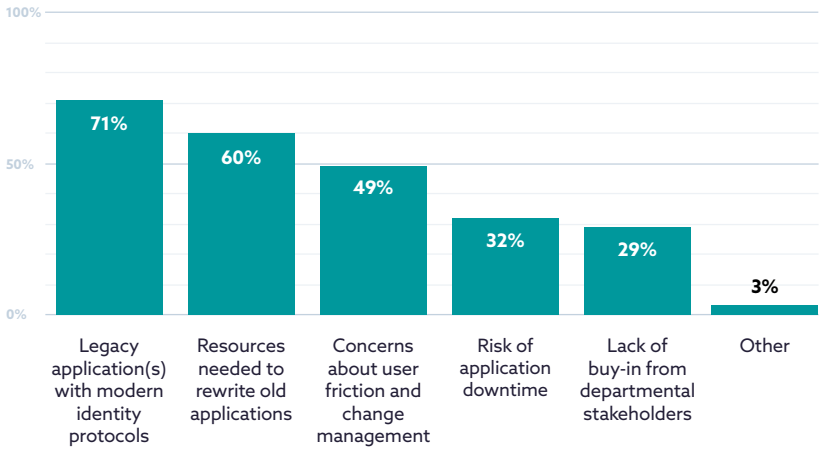
Top challenges organizations face in modernizing IAM architecture.



Level of difficulty with onboarding on-premises applications to a cloud IDP.

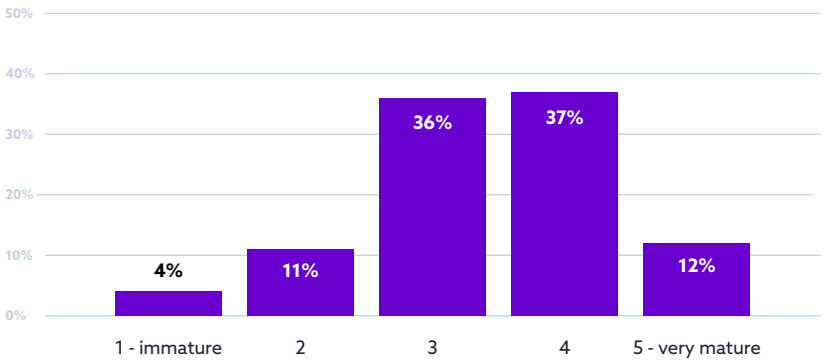


Barriers to deploying advanced authentication for all applications.

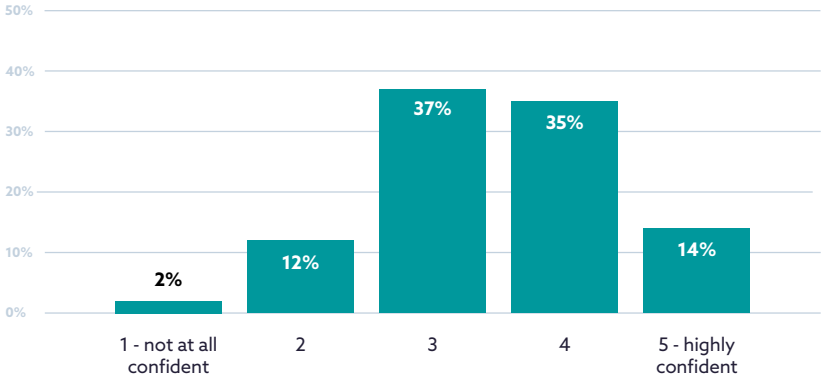


Identity Continuity and Resilience

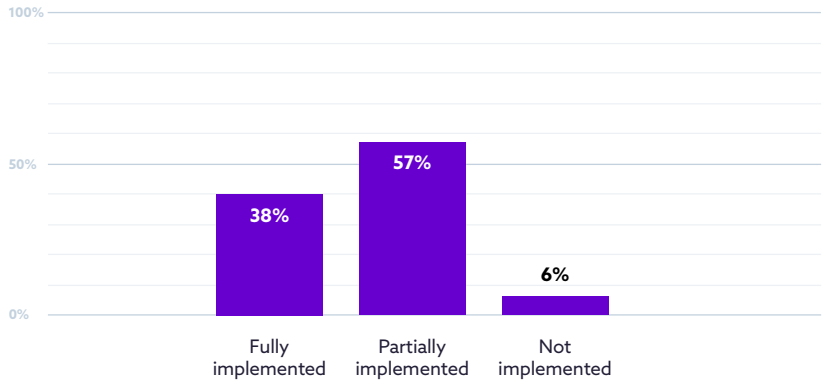
Maturity of organizations' identity resilience and continuity program.



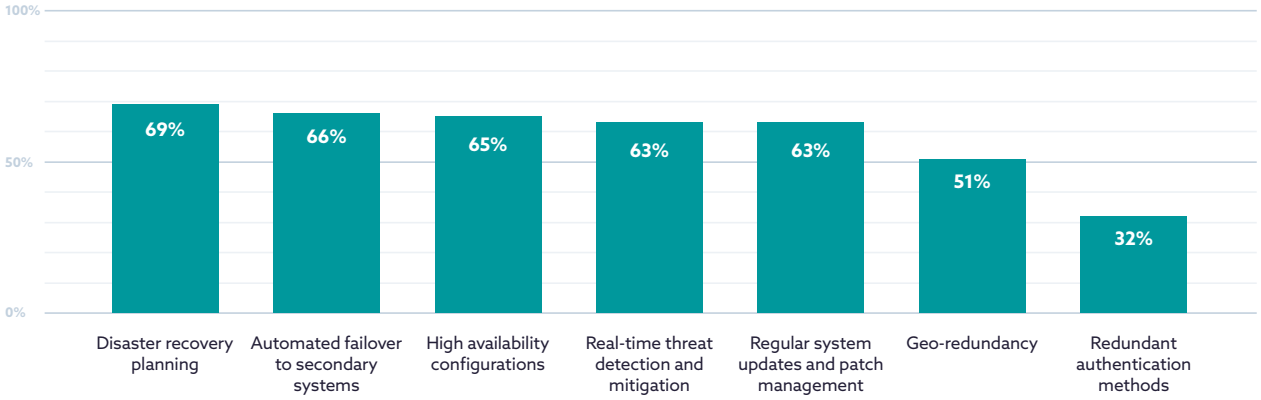
Confidence in organizations' IAM infrastructure ability to withstand and recover from identity outages, disruptions, or attacks.



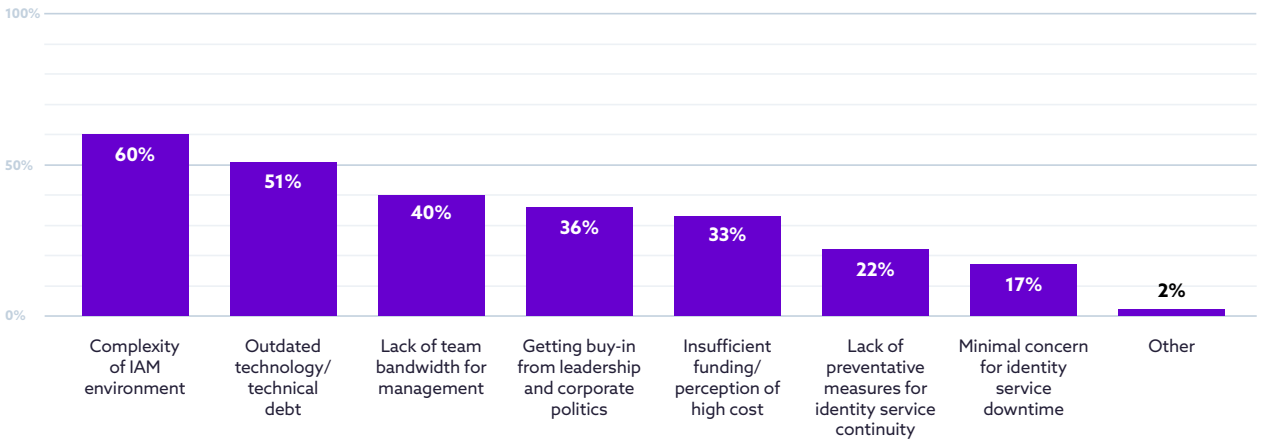
Status of Solution Implementation for Continuous Availability of Identity Services



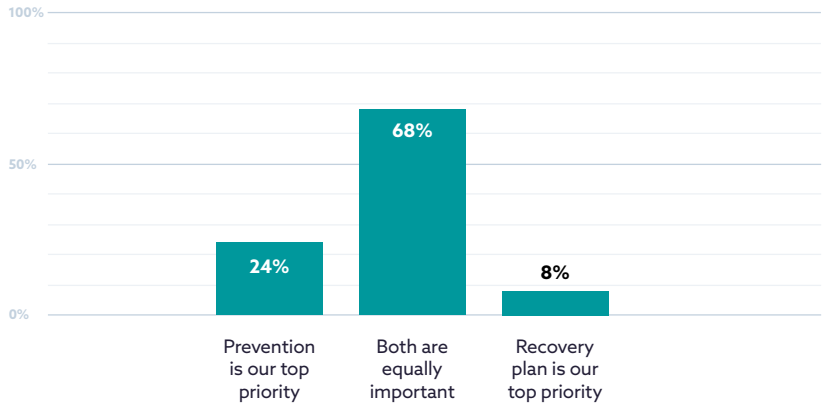
Preventative measures organizations employ to ensure continuous availability of identity services.



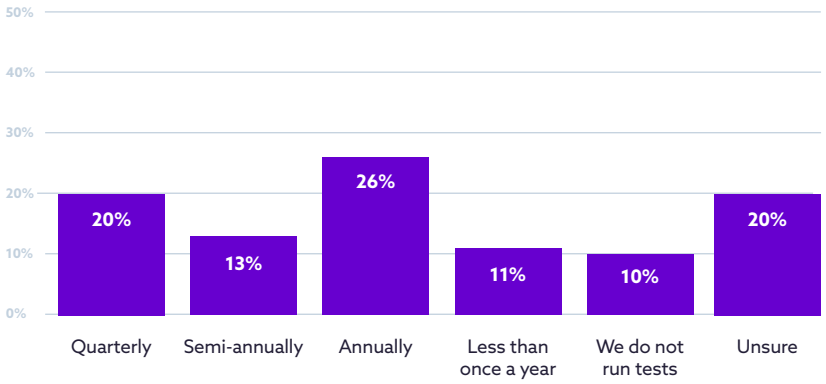
Challenges organizations have in achieving a resilient identity infrastructure.



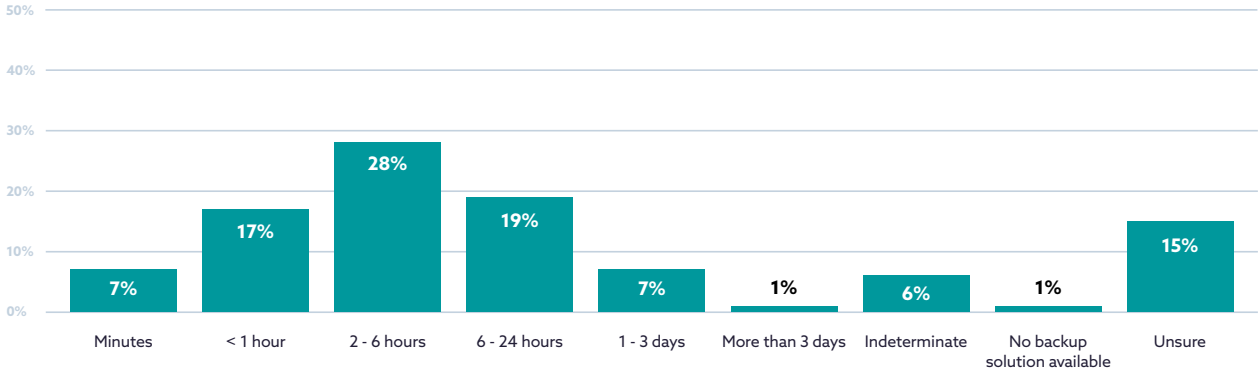
Prioritization of Preventing Downtime vs. Recovery Planning for Identity Services



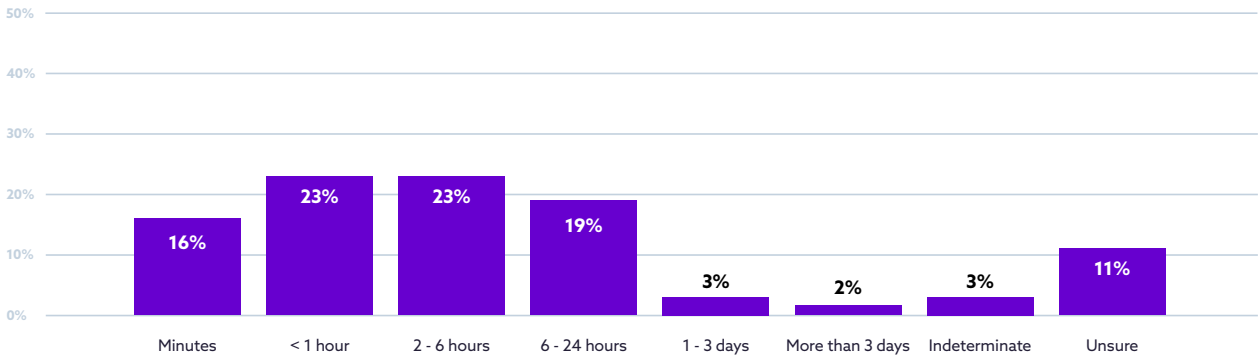
Frequency of end-to-end tests on organizations identity resilience program.



Time table to maintain service continuity in the event of a disruption.

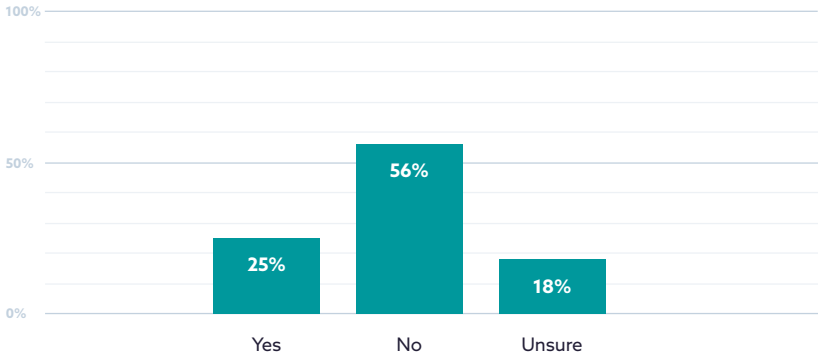


Time organizations can afford to have their primary identity service down for.

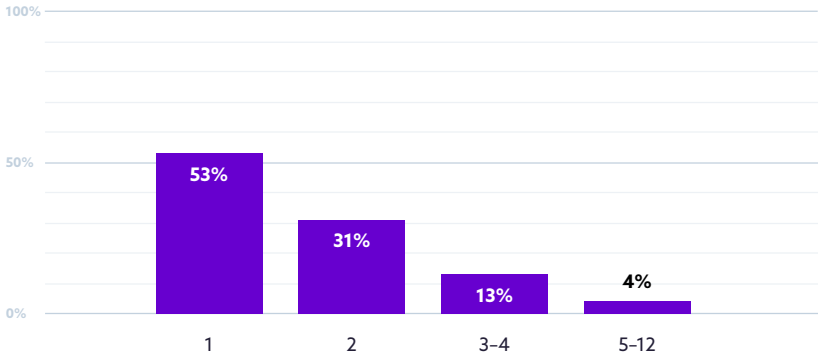


Outages and Disruptions

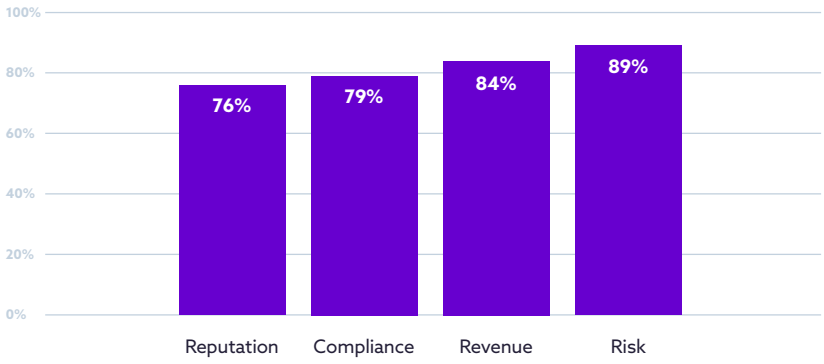
Organizations' business operations interrupted due to inavailability of cloud identity services.



Number of times primary identity service had an outage in the past year.

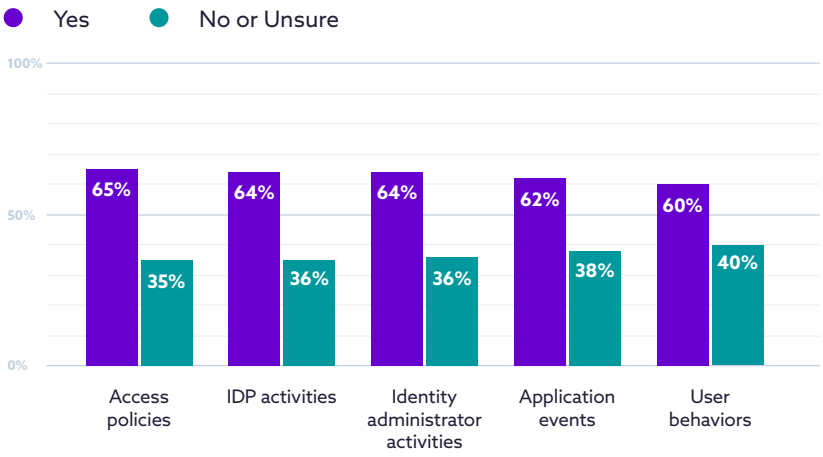


Areas organizations experienced no impact due to their outage.

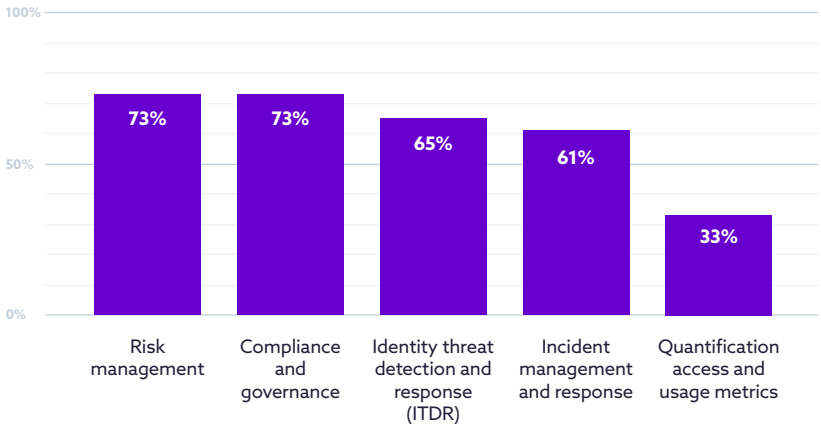


Identity Analytics

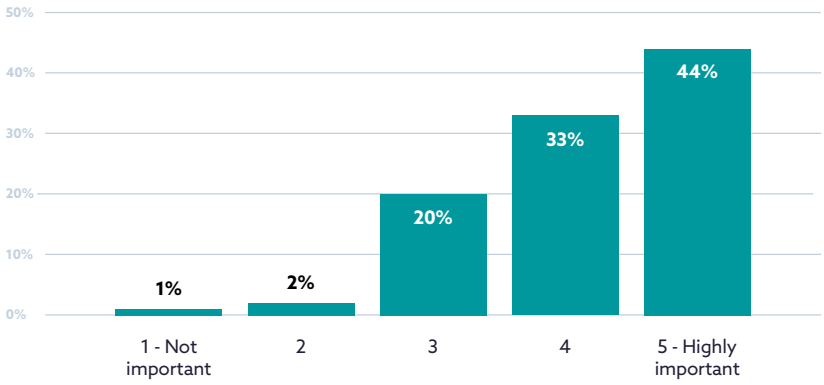
Does your organization have visibility into the follow items?



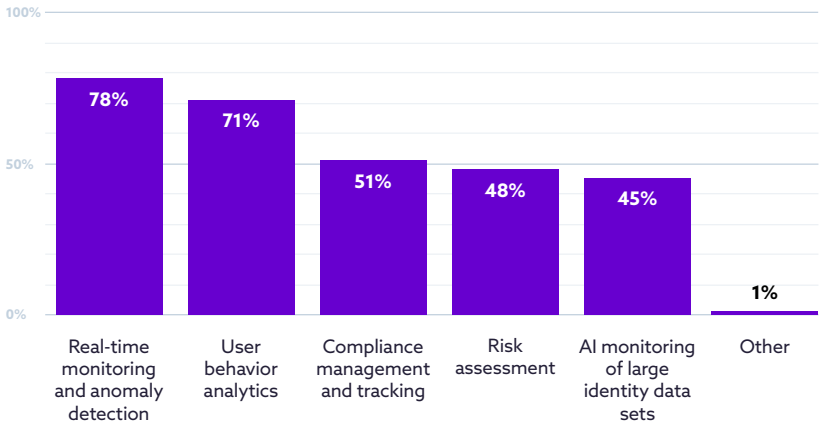
Reasons organizations require better visibility.



Importance of analytics that provide visibility into organizations' IAM environments.

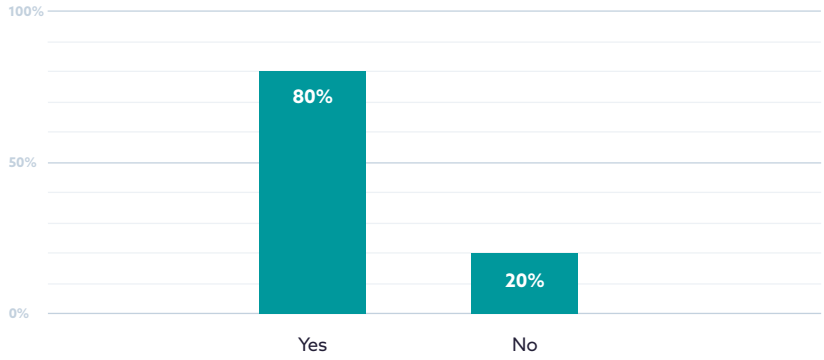


Analytical capabilities needed to improve identity management.

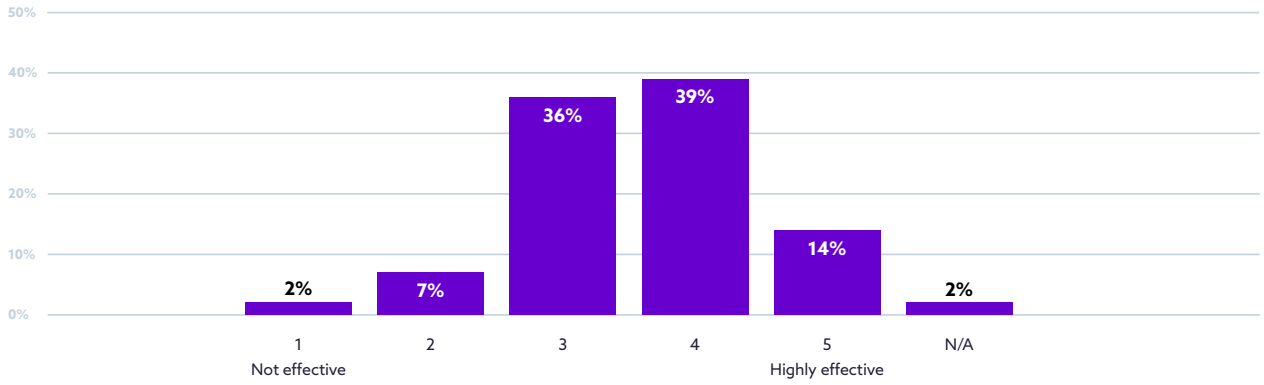


Application Identity Governance

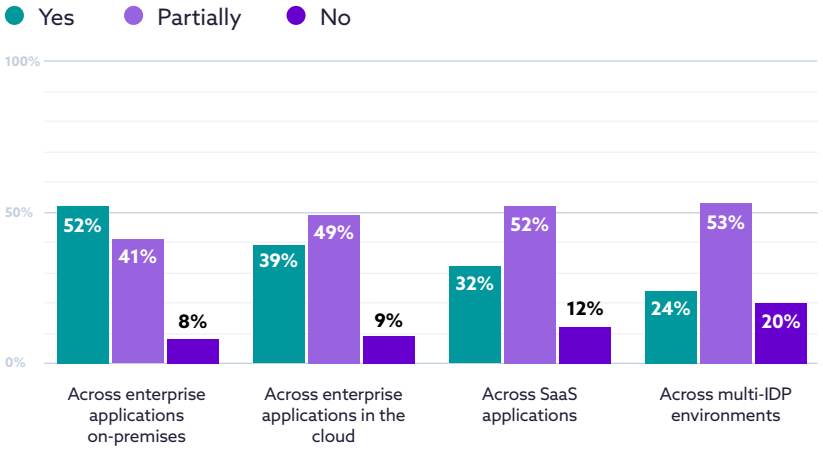
Organization is able to maintain compliance with all the regulations related to identity management for their applications.



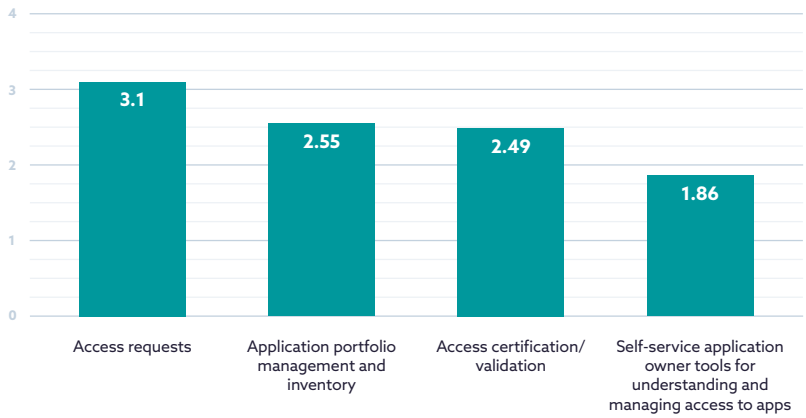
Effectiveness of organizations' identity governance approach to managing application identity and access, specifically for application owners.



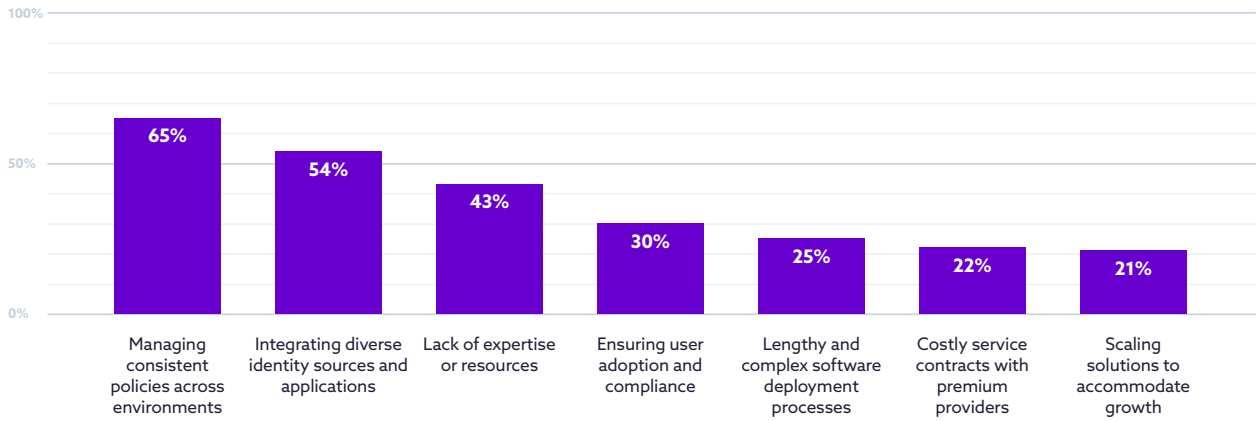
Are Identity Governance tools meeting organizations' needs in these areas?



Identity governance use cases ranked most to less relevant to organization's needs for managing applications.

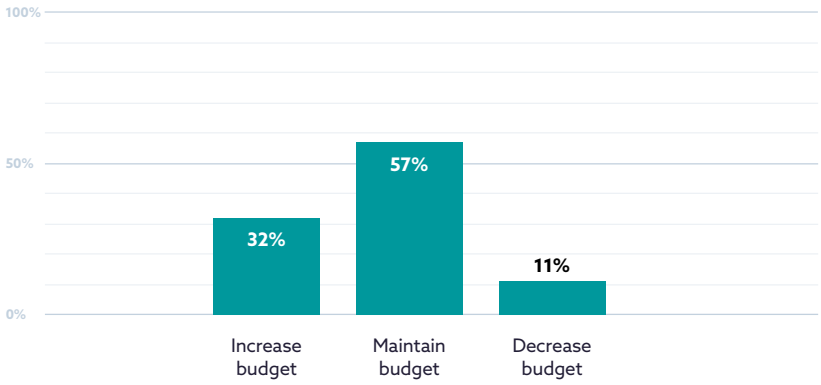


Primary challenges organizations face in implementing identity governance solutions across applications.

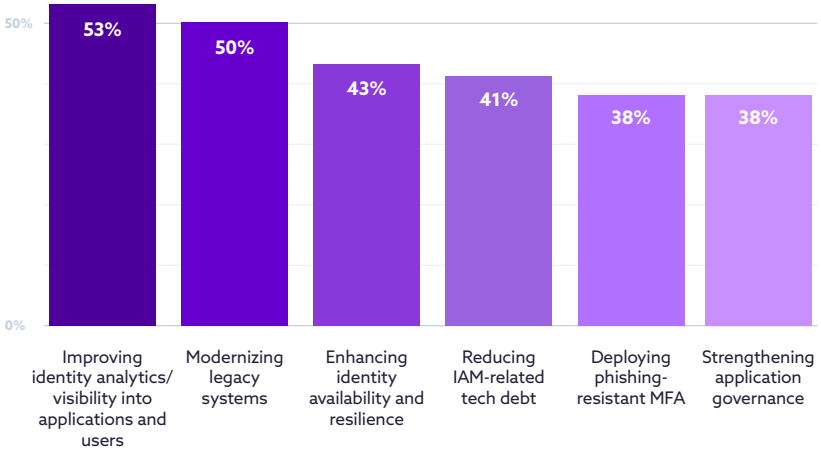


Future of Directions and Investments

Anticipated budget changes for identity management solutions in the next 12 months.



Prioritized areas of identity and access management for future investment.

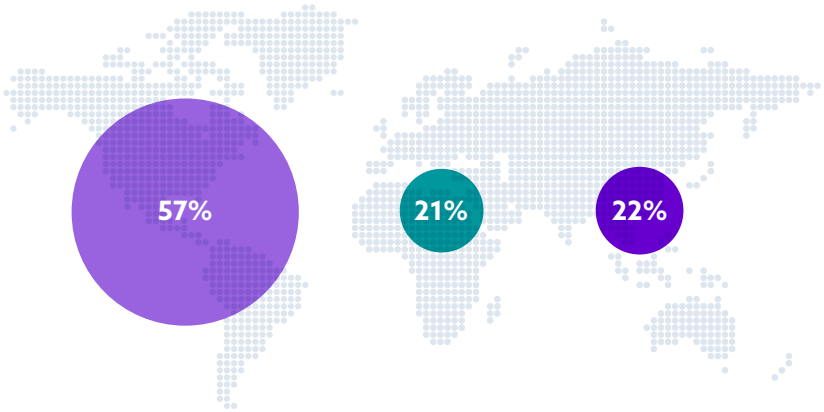


Demographics

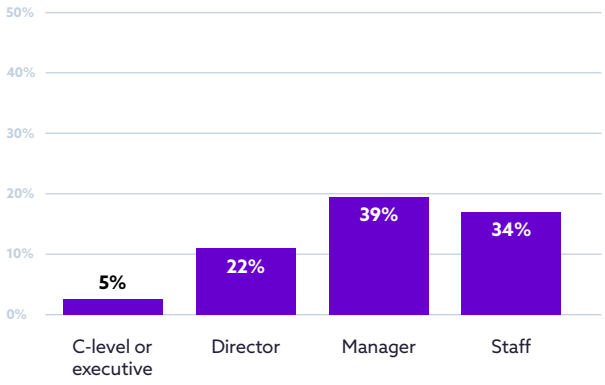
The survey was conducted online by CSA in June/July 2024 and received a total of 950 responses from IT and security professionals from organizations of various sizes and locations.

What region of the world are you located in?

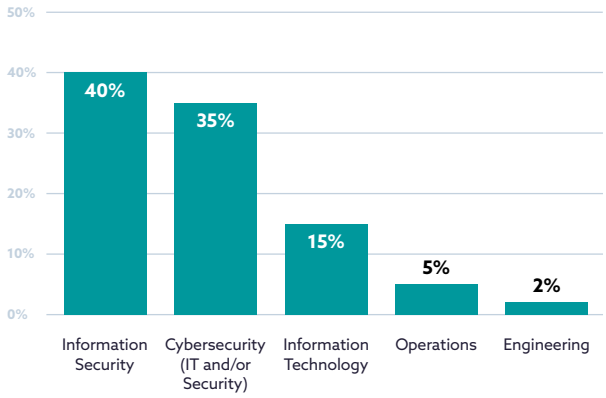
- Americas
- Europe, Middle East, Africa (EMEA)
- Asia-Pacific (APAC)



What best describes your job level?



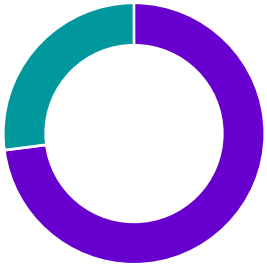
Which of the following best describes your current department?



Which of the following best describes the principal industry of your organization?

30%	Telecommunications, Technology, Internet & Electronics	1%	Automotive
24%	Finance & Financial Services	1%	Business Support & Logistics
7%	Healthcare & Pharmaceuticals	1%	Agriculture
7%	Government	1%	Construction, Machinery, and Homes
5%	Manufacturing	1%	Entertainment & Leisure
5%	Prefer not to answer	1%	Real Estate
3%	Health & Fitness	1%	Transportation & Delivery
3%	Retail & Consumer Durables	1%	I am currently not employed
3%	Insurance	0%	Advertising & Marketing
2%	Airlines & Aerospace (including Defense)	0%	Food & Beverages
2%	Utilities, Energy, and Extraction	0%	Nonprofit
1%	Education		

Estimate the annual revenue for your organization.



- **73%** $1 billion-plus
- **27%** $500 million to $999 million

Survey Creation and Methodology

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to widely promote best practices and ensure cybersecurity in cloud computing and IT technologies. CSA also educates various stakeholders within these industries about security concerns in all other forms of computing. CSA's membership is a broad coalition of industry practitioners, corporations, and professional associations. One of CSA's primary goals is to conduct surveys that assess information security trends. These surveys provide information on organizations' current maturity, opinions, interests, and intentions regarding information security and technology.

Strata Identity commissioned CSA to develop a survey and report to better understand the industry's knowledge, attitudes, and opinions regarding multi-cloud identity security trends and challenges. Strata Identity financed the project and co-developed the questionnaire with CSA research analysts. The survey was conducted online by CSA in June/July 2024 and received a total of 950 responses from IT and security professionals from organizations of various sizes and locations. CSA's research analysts performed the data analysis and interpretation for this report.

Goals of the Study

The primary objectives of the survey were to gain a deeper understanding of several critical aspects of multi-cloud identity security:

- The state of identity architecture in the enterprise
- Identity continuity and resiliency plans
- Gaps in identity analytics capabilities
- Current approach to identity governance for applications