EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Prepared for:

Omada

# Navigating the Identity Crisis:

## A Data-Driven Analysis of IGA Maturity, Risks, and Future Roadmaps

**January 2026 EMA Research Report**
By Ken Buckler, Research Director
*Information Security, Risk, and Compliance Management*

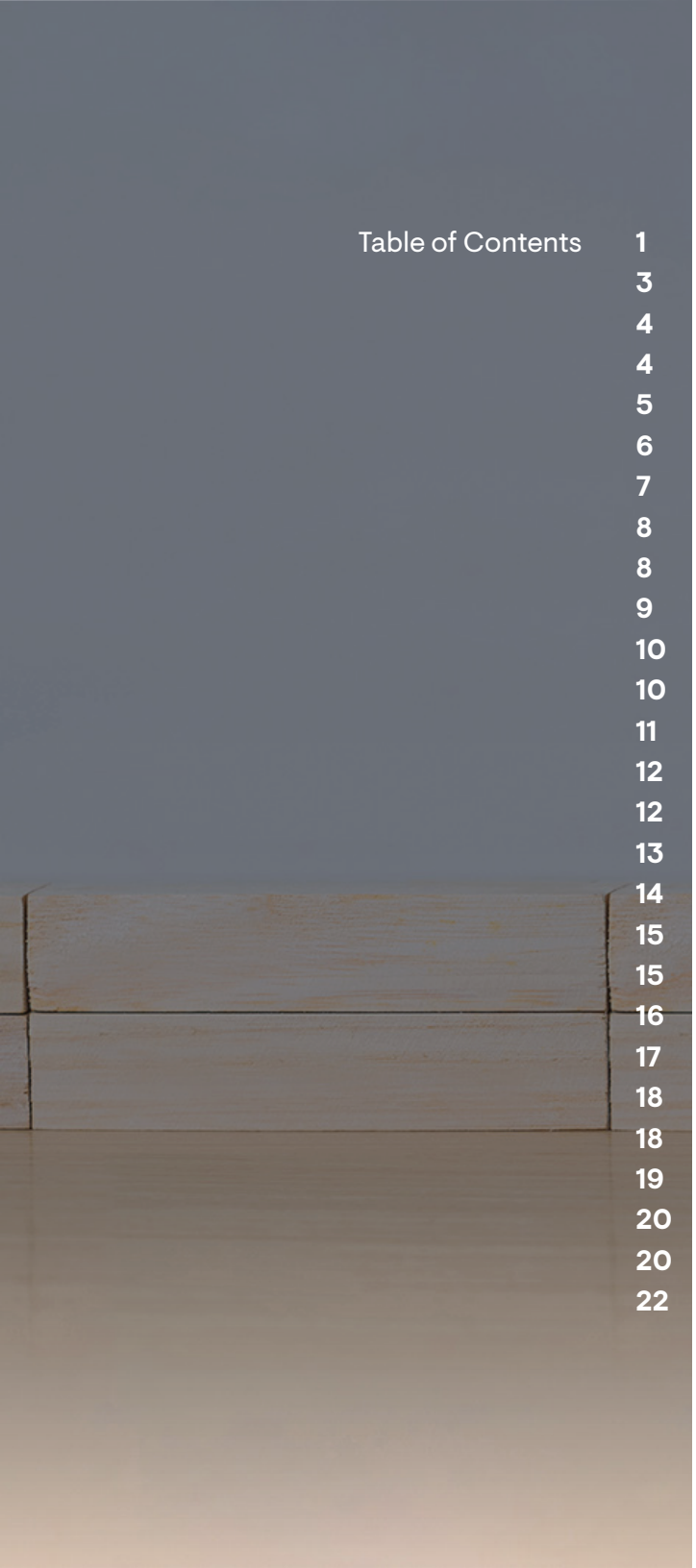


Table of Contents


# Introduction

Identity governance and administration (IGA) serves as the definitive framework for managing the lifecycle of user access and policy enforcement. By ensuring that only authorized personnel interact with sensitive systems, IGA significantly reduces the risk of data breaches and establishes the necessary foundation for zero trust architecture. Organizations invest in these solutions to mitigate insider threats and automate the rigorous documentation required for regulatory compliance. This automation also drives operational performance by streamlining onboarding processes and reducing the administrative burden on IT teams.

Despite these clear objectives, the practical reality of implementation often lags behind strategic intent. EMA's recent survey data indicates that while security remains the primary driver for adoption, 30% of organizations have abandoned or scaled back their programs due to persistent challenges. This research report examines the friction points between legacy infrastructure and modern demands to reveal the specific gaps in identity lifecycle management.

This report provides a critical examination of the current state of identity governance and administration, exposing the tension between the necessity of robust security measures and the operational realities organizations face today. While IGA is universally recognized as essential for compliance and risk management, a significant disconnect remains between strategic intent and execution. This gap is evidenced by the fact that 30% of organizations have been forced to abandon or scale back their zero trust programs, signaling a profound mismatch between solution capabilities and organizational needs. Furthermore, despite the market's aggressive push toward SaaS, 55.6% of enterprises continue to embrace on-premises or private cloud systems. The following analysis explores why these implementations fail, identifies specific risks in identity lifecycle management, and charts a roadmap toward a modern, automated, and AI-driven identity fabric.


# The Current State of IGA Deployment

# Demographics & Landscape

EMA surveyed 135 IT decision makers and practitioners regarding their usage of identity governance solutions. These organizations had 750 or more employees and came from a diverse sampling of industries. Over 86% of respondents indicated that identity governance is "very important" to their organization.

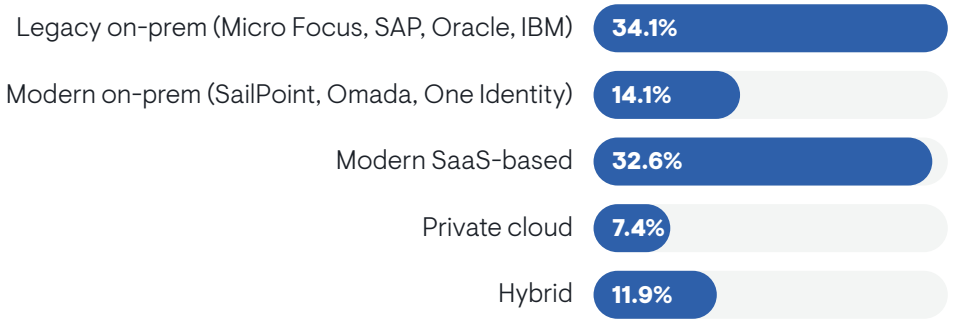
**How important is identity governance to your organization?**

**86.7%** | Very important **13.3%** | Somewhat important

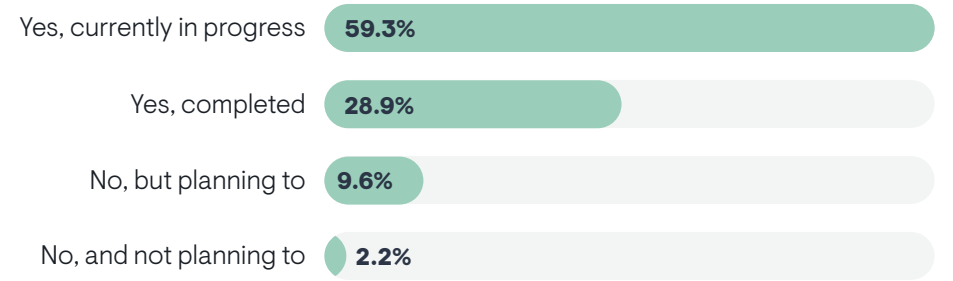
# Cloud vs. On-Premises Reality

The identity governance landscape presents a stark contrast between the market's "cloud-first" narrative and the persistent reality of on-premises infrastructure. Despite the industry-wide push toward SaaS, over half of organizations continue to rely on on-premises or private cloud systems, with legacy on-prem platforms alone accounting for the largest share of deployments at 34.1%. However, this footprint does not indicate stagnation, but rather a massive ongoing migration. While only 2.2% of organizations have no plans to modernize, a commanding 59.3% are actively in the process of transitioning their legacy environments to modern solutions.

**What type of IGA system are you primarily using?**

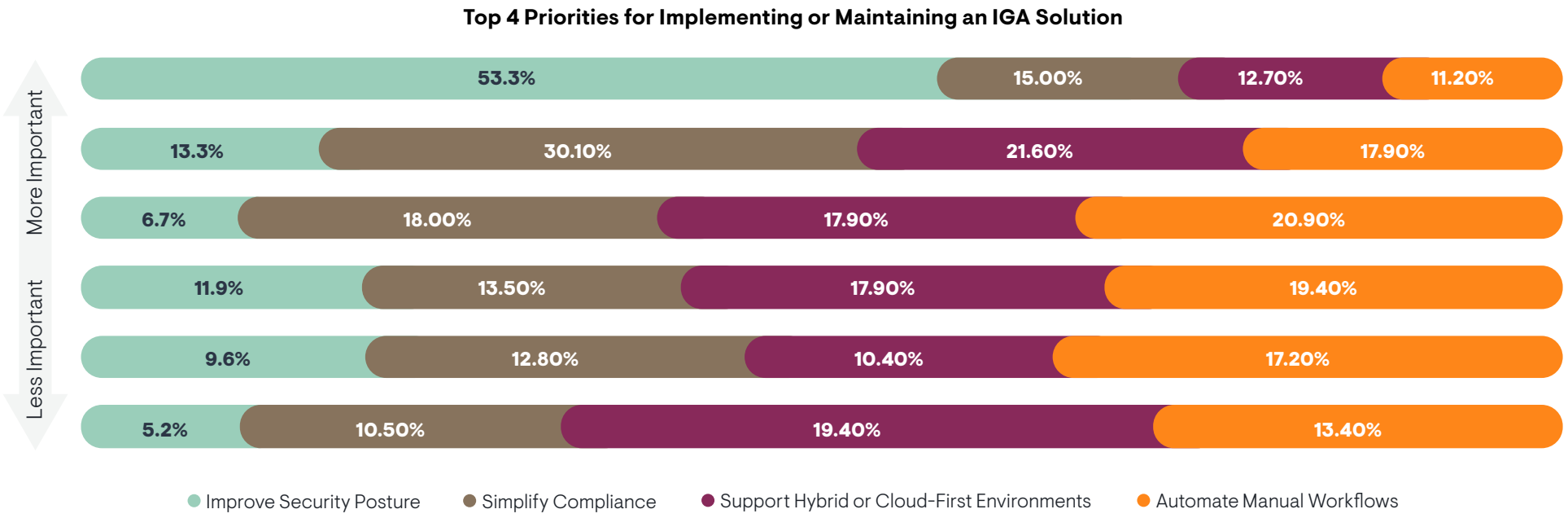



**Is your organization transitioning from a legacy or homegrown IGA system to a modern one?**



# Drivers for Adoption

The motivation for implementing identity governance and administration has shifted decisively toward active risk mitigation, with security posture emerging as the undisputed primary driver. Data reveals that 53.3% of organizations rank improving security posture as their single most important priority, far outstripping all other objectives and establishing it as the foundational requirement for modern identity strategies. Close behind this security mandate is the critical need to navigate regulatory complexity, with simplifying compliance and audit processes serving as the dominant secondary objective, selected by 30.1% of respondents. This hierarchy of needs—placing active security defense ahead of passive regulatory adherence—signals that organizations are moving beyond compliance as a mere administrative "box-checking" exercise and are instead deploying IGA to seek genuine, quantifiable risk reduction.

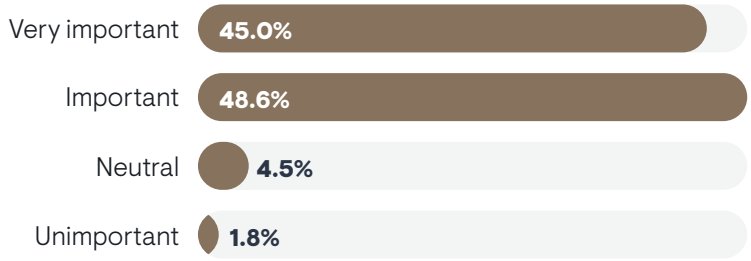


# Defining Key Identity Governance Principles

# Role-Based Access Control (RBAC)

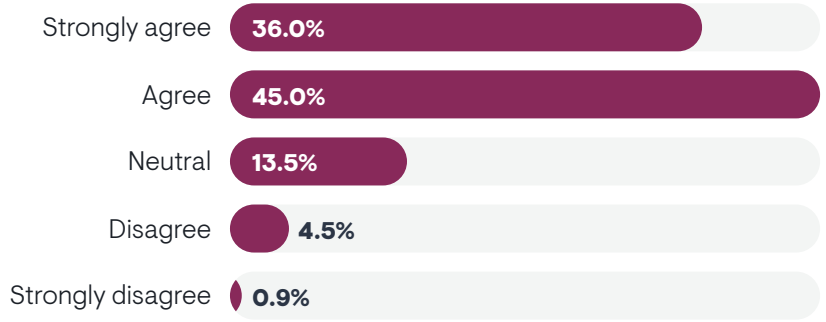
Role-based access control (RBAC) endures as a foundational element of modern identity governance, designed to automate permission adjustments during employee transitions and thereby prevent unauthorized access stemming from outdated roles. The strategic necessity of this mechanism is universally recognized; survey data confirms that an overwhelming 93.6% of organizations consider RBAC either important or very important to their governance strategy, with only a negligible 1.8% dismissing its significance. This consensus underscores that despite the emergence of newer frameworks, the ability to align access rights dynamically with job functions remains a non-negotiable requirement for securing the identity lifecycle.

**How important is role-based access control (RBAC) in your identity governance strategy?**




Least-privilege functions as the operational core of zero trust, ensuring that users retain only the minimum access necessary to perform their duties. This principle is not merely a theoretical best practice, but also a widely accepted security imperative. Survey data confirms that 81% of organizations agree or strongly agree that implementing least-privilege policies decreases security risks. This overwhelming consensus highlights that verifying every access request is no longer optional, but is viewed as a critical control for minimizing the blast radius of potential breaches.

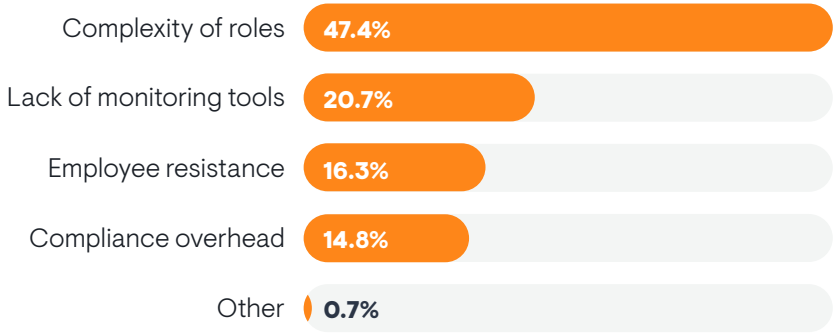
**To what extent do you agree that implementing least-privilege policies decreases security risks?**



# Separation of Duties (SoD)

Managing separation of duties remains one of the "biggest challenges" for respondents, especially due to the complexity of roles. This critical control method to prevent conflict of interest and fraud cannot be successful if separation of duties is not properly implemented.

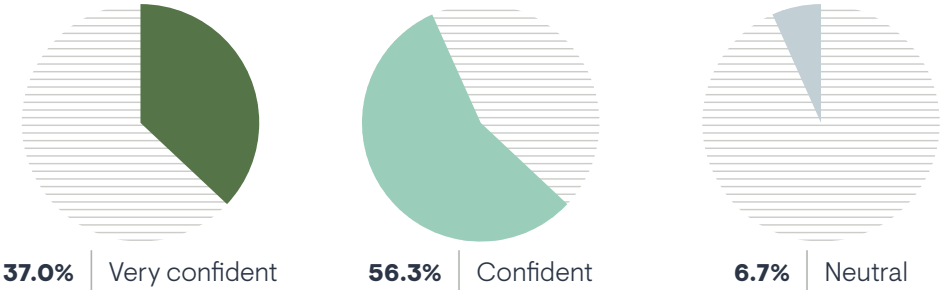
**What is your biggest challenge in managing separation of duties (SoD)?**




# Entitlement Management

Granular oversight of user privileges remains a challenge for modern enterprises, with confidence levels in entitlement management exposing a notable risk gap. While 56.3% of organizations report feeling confident in their practices, this assurance is often superficial. Only 37% of respondents possess the high degree of certainty required to classify themselves as very confident, indicating that the majority of IT teams likely lack the deep visibility needed to effectively audit and control complex entitlements.

**How confident are you in your current entitlement management practices?**

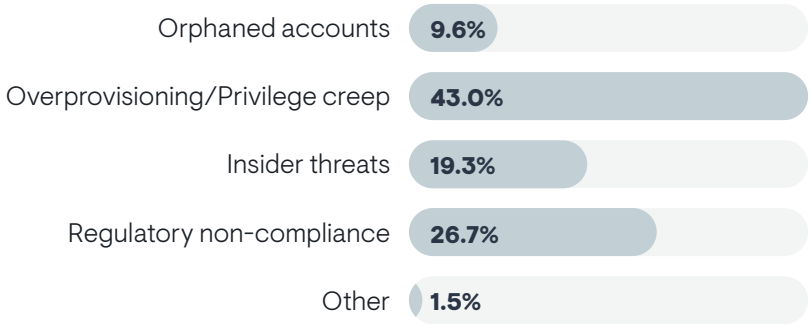



# Primary Risks to Identity Lifecycle Management

# The Risk Landscape

The risk landscape for identity lifecycle management is multifaceted, necessitating robust strategies to mitigate insider threats, protect sensitive PHI/PII data, and manage the expanding attack surface of non-human identities, like bots and service accounts. However, when organizations identify their most pressing immediate risk, the data reveals that overprovisioning and privilege creep are the dominant concerns, cited by 43% of respondents—more than double the number who prioritized insider threats (19.3%). This suggests that while malicious intent and regulatory non-compliance (26.7%) are critical high-level fears, the day-to-day operational reality is that organizations are struggling most with "access sprawl," in which users accumulate excessive permissions that go unchecked.

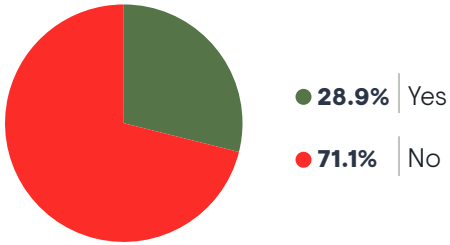
**Which of the following risks is the most pressing for your organization today?**

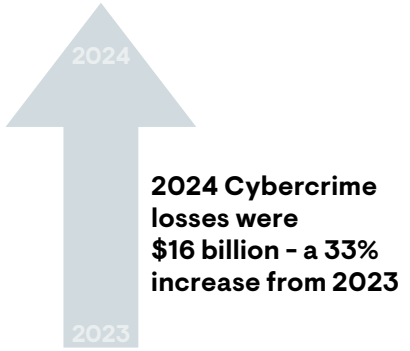



# The Cost of Failure

According to the FBI, cybercrime financial losses increased in 2024 by 33%, with a total estimated loss of $16 billion. While exact causes of these incidents are not readily available, the OWASP Top 10 has consistently listed "broken access controls" as the top application security risk, with 94% of the applications OWASP tested having some form of broken access control. Since 28.9% of organizations EMA surveyed experienced a breach incident involving a compromised identity in the past year, failing to properly implement identity governance is a critical problem.

**Have you experienced a breach or incident involving a compromised identity in the past year?**



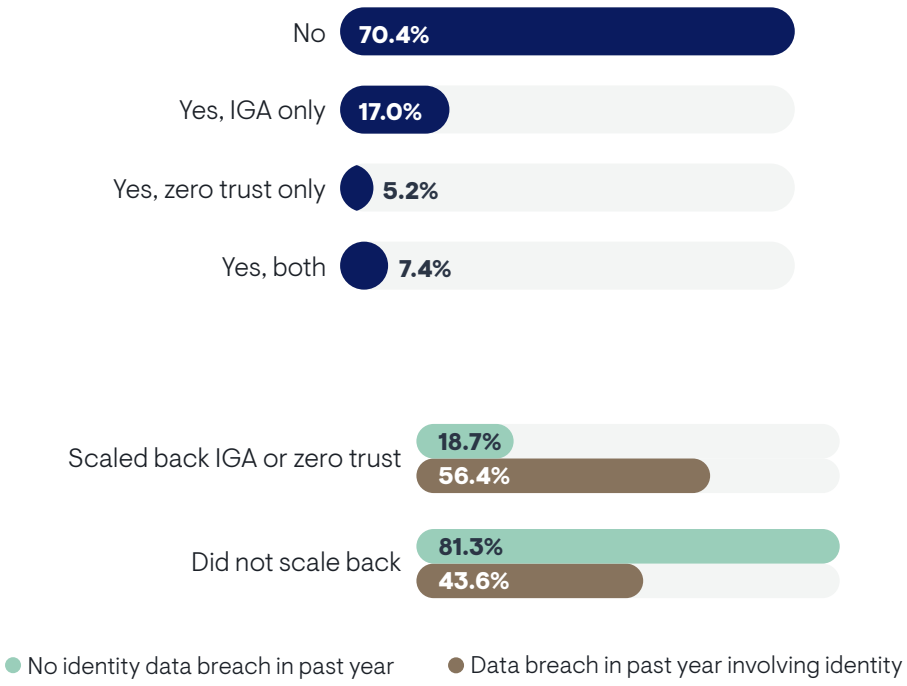

(Source: FBI Internet Crime Complaint Center)


# Identifying Gaps in IGA Deployment (The “Why” Behind Failure)

# The 30% Failure Rate

With identity as a foundational pillar of zero trust security maturity, it becomes more urgent than ever that organizations implement robust identity governance programs. By itself, the statistic that 30% of organizations have abandoned or scaled back programs is extremely concerning, but the numbers get worse when analyzing organizations that had to abandon or scale back their IGA or zero trust programs. Just over 56% of organizations experienced a data breach in the past year and scaled back their programs.

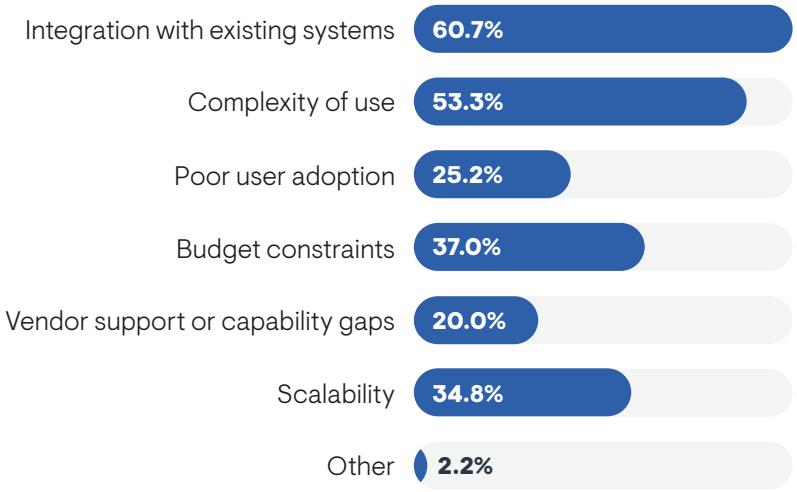
**Have you abandoned or scaled back your IGA or zero trust programs?**




# Common Problems

Significant operational friction, primarily centering on technical interoperability and user experience, frequently obstructs the path to effective identity governance. The most pervasive challenge, reported by a staggering 60.7% of organizations, is the difficulty of integrating IGA solutions with existing systems. This "integration fatigue" suggests that many tools operate as isolated silos rather than seamless connectors within the broader IT ecosystem. Compounding this issue is the sheer complexity of use, cited by 53.3% of respondents as a major hurdle. When solutions are overly intricate, they create administrative burdens that often lead to "rubber stamping" access reviews rather than enforcing genuine governance. While budget constraints (37%) and scalability concerns (34.8%) persist, the data clearly indicates that the primary barriers to success are functional: tools that are simply too difficult to connect and too complex to operate effectively.

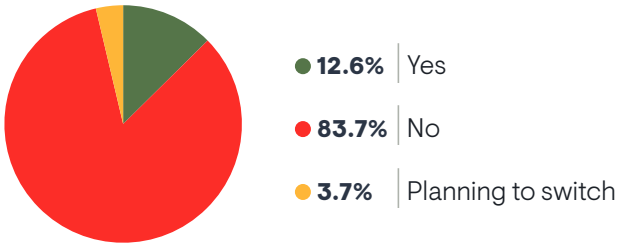
**What challenges are you facing in your IGA journey?**



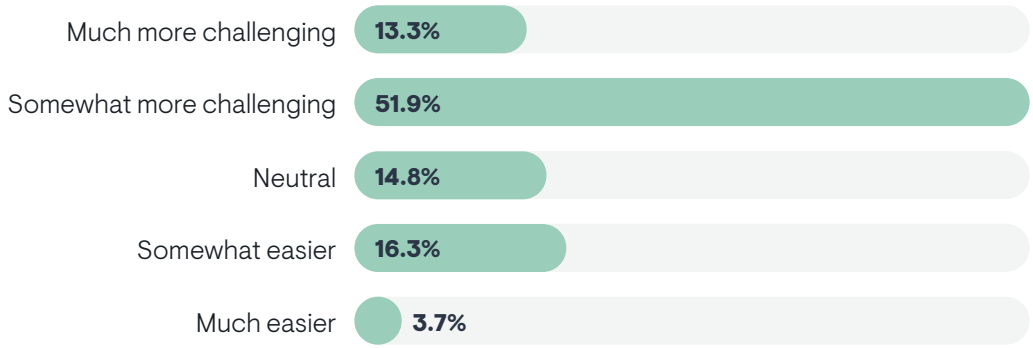
# The User Experience & Integration Gap

Dissatisfaction with IGA capabilities has translated into tangible market movement, with 12.6% of organizations switching vendors in the past two years specifically due to performance issues. This churn is heavily influenced by the operational strain of distributed workforces; a combined 65.2% of respondents reported that remote work made their identity governance operations more challenging, creating a pressure cooker environment where legacy tool inefficiencies are no longer tolerable. When viewed alongside the 60.7% of users struggling with integration fatigue, it becomes clear that the inability of existing solutions to bridge the gap between complex internal demands and the flexibility required by remote environments often drives the decision to switch.

**Have you switched IGA vendors in the past two years due to dissatisfaction?**




**How has remote work impacted your identity governance operations?**

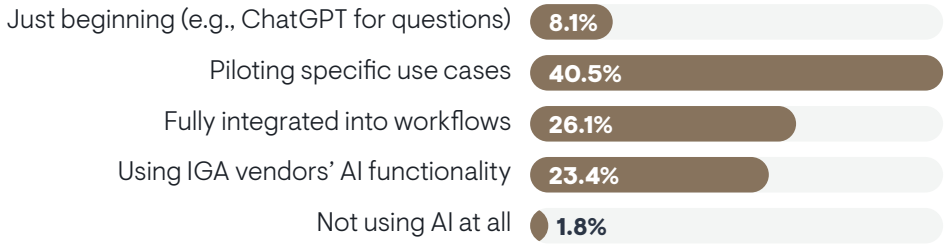



# The Role of Automation and AI in Closing the Gap

# Current Maturity

A distinct gap between intent and execution defines the current landscape of automation and AI in identity governance. While the drive for operational efficiency is nearly universal—with a combined 93.6% of organizations rating the ability to automate governance processes as either extremely or very important—actual AI maturity remains largely experimental. The majority of organizations are currently in a "test and learn" phase, with 40.5% piloting specific use cases rather than deploying comprehensive solutions. However, the trajectory is clear; with only 1.8% of respondents not using AI at all and 26.1% already reporting full integration into workflows, the market is rapidly moving past initial hesitancy toward a future in which intelligent automation is a standard operational requirement.

**How would you describe your organization's maturity in using AI for identity-related decisions?**

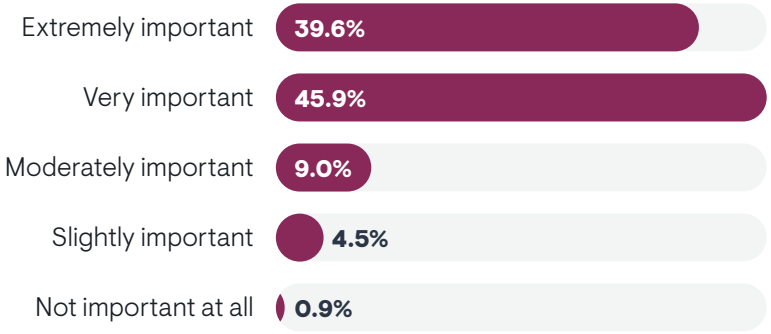



**How important is the ability to automate identity governance processes to your organization's operational efficiency?**


# The Promise of AI

The promise of AI in identity governance lies in its ability to transform static administration into dynamic, intelligent defense. By leveraging smart analytics for anomaly detection, organizations can automatically identify privilege creep and receive proactive recommendations for access changes that might otherwise go unnoticed by human reviewers. Beyond security insights, AI delivers critical operational efficiency by automating provisioning and deprovisioning workflows, effectively reducing the manual data entry that is frequently responsible for costly errors. This capability is no longer viewed as a futuristic luxury, but as an immediate necessity, evidenced by the fact that a combined 85.5% of organizations now rate AI functionality as either extremely or very important to their IGA solutions.

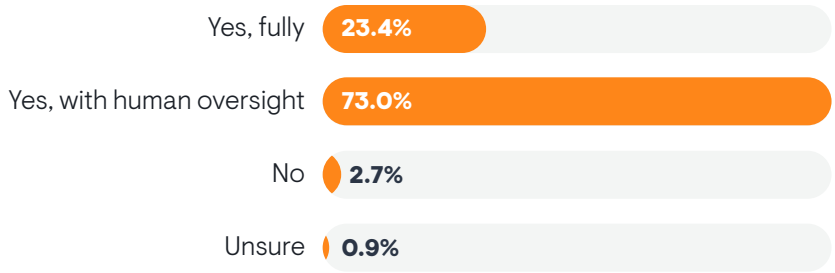
**How important is AI functionality in an IGA solution today?**



# The Trust Factor

Despite the clear operational benefits of artificial intelligence, organizations exhibit significant caution regarding the deployment of fully autonomous agents for identity decisions. The survey data illuminates a distinct "trust boundary," where only 23.4% of respondents are willing to fully trust an agentic AI to manage their environment without intervention. In stark contrast, a commanding 73% of organizations insist on maintaining human oversight, signaling that while the market is eager to adopt AI as a sophisticated decision support tool, the leap to unsupervised "autopilot" governance remains a bridge too far for the majority of security leaders.

**Would you trust an agentic AI (e.g., an autonomous AI assistant) to manage identity decisions in your environment?**

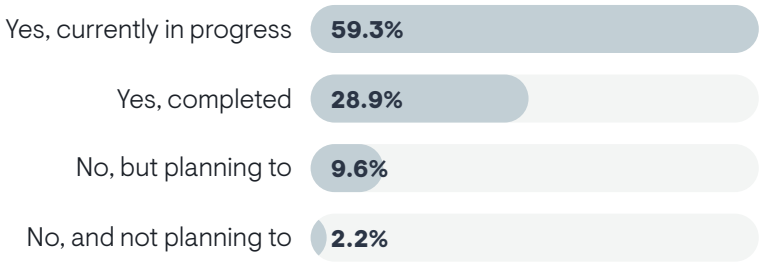



# Operational Efficiency & Cost Optimization

# Business Case for Modernization

The business case for IGA modernization is fundamentally rooted in the dual necessity of resource optimization and error reduction. By automating complex role assignments, organizations can simultaneously liberate IT resources for critical security tasks and eliminate the human errors that often create security gaps. The market clearly recognizes this imperative, as evidenced by the massive wave of infrastructure renewal currently underway. A commanding 59.3% of organizations is currently in the process of transitioning from legacy or homegrown systems, while another 28.9% already completed the journey. This leaves a negligible 2.2% of organizations with no plans to modernize, effectively isolating them as outliers in an industry rapidly converging on automated, scalable identity fabrics.

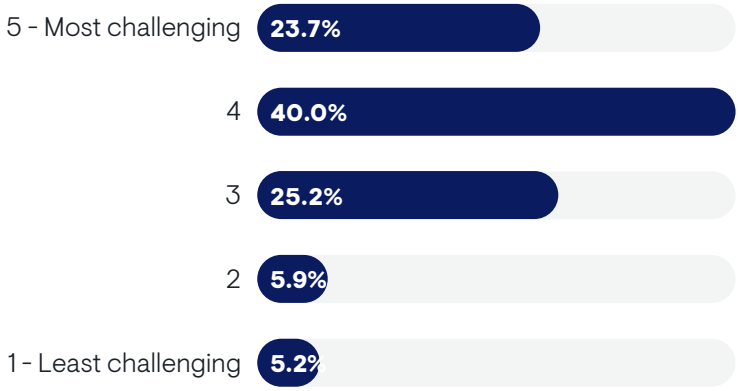
**Is your organization transitioning from a legacy or homegrown IGA system to a modern one?**




# Scalability

As organizations expand, the demand for identity governance solutions that can scale effectively without introducing debilitating complexity becomes paramount. However, the data reveals that achieving this elasticity is a significant operational hurdle for the majority of enterprises. When asked to rate the difficulty of scaling their current IGA solution for growth, a combined 63.7% of respondents indicated a high level of challenge (rating it a 4 or 5), with nearly one quarter (23.7%) describing it as the "most challenging" aspect of their implementation. This friction threatens to undermine the long-term cost efficiencies that governance is intended to deliver, creating a barrier to the reduced compliance costs and mitigated breach risks that justify the investment in the first place.

**How challenging was it to get your current IGA solution scaled for growth?**



# Strategic Recommendations for IGA Success

# Best Practices

Foundational to any successful IGA deployment is the establishment of vendor-agnostic best practices, a strategic necessity that ensures governance standards are dictated by internal security requirements rather than external vendor marketing. While 53.2% of organizations have successfully defined these independent guideposts, a significant 38.7% are operating with only partial frameworks and 8.1% lack them entirely. This gap indicates that nearly half of all organizations are at risk of allowing tool capabilities to dictate their security strategy rather than having a predefined governance model driving their technology selection.

**Do you feel your organization has vendor-agnostic best practices to guide your IGA project success?**

**53.2%** | Yes

**8.1%** | No

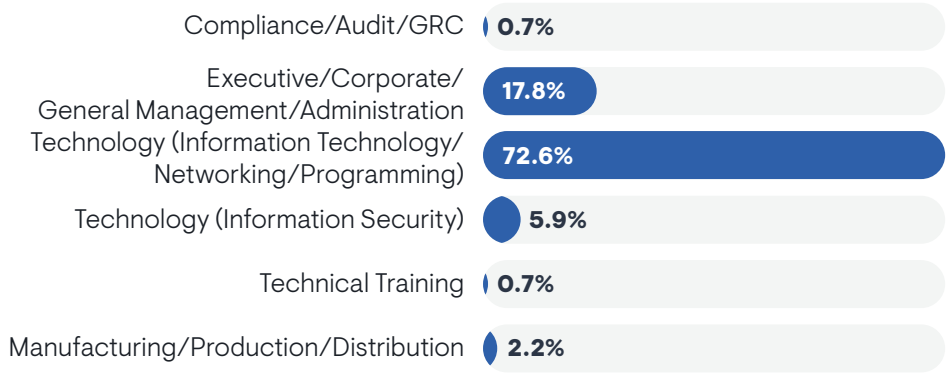
**38.7%** | Partially

# Conclusion & Future Outlook

Identity governance and administration currently stands at a decisive crossroads, caught between entrenched legacy infrastructure and the urgent demand for modern agility. While 55.6% of organizations continue to rely on on-premises or private cloud solutions, the cracks in legacy solutions are becoming undeniable, evidenced by the 30% of enterprises that were forced to abandon or scale back their programs due to operational failures. However, this dissatisfaction is driving a massive wave of renewal rather than resignation. With 59.3% of organizations actively transitioning to modern systems, the market is decisively rejecting the static, siloed approaches of the past in favor of dynamic platforms capable of supporting hybrid environments.

Looking ahead, the evolution of IGA will be defined by the successful integration of artificial intelligence and automated lifecycle management to bridge the gap between security mandates and user experience. As organizations move beyond seeing governance as a mere compliance burden, the adoption of AI-driven insights—already underway in over 66% of organizations in some form—will become the standard for achieving a true zero trust posture. Ultimately, the organizations that succeed will be those that transform identity from a back-office administrative task into a proactive security enabler, leveraging automation to reduce risk while simultaneously unlocking operational speed.

**Which of the following best describes the department or functional area in which you work?**

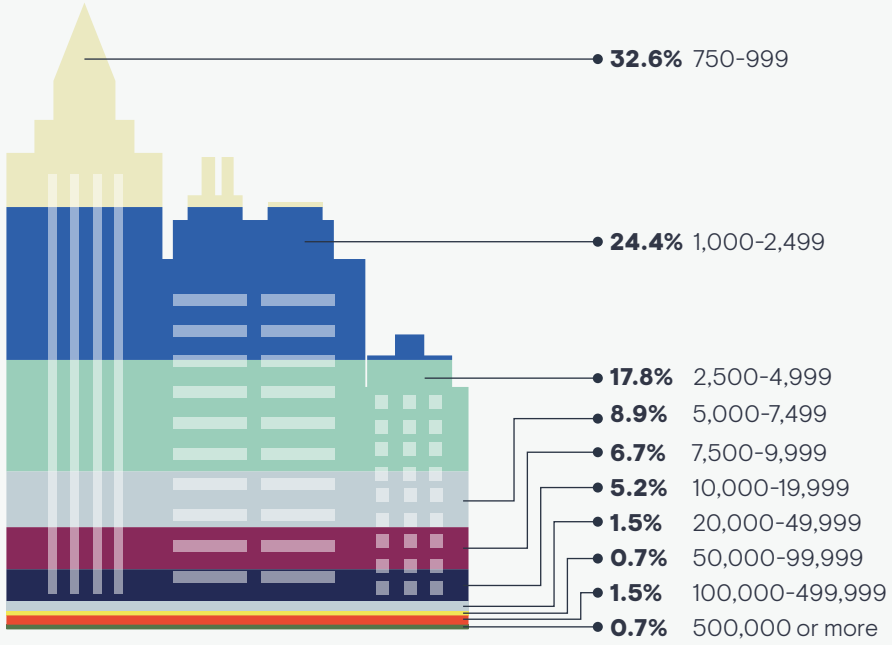


**Omada is a leader in identity security and governance, helping organizations reduce risk by securing access for every identity, human and non-human.**

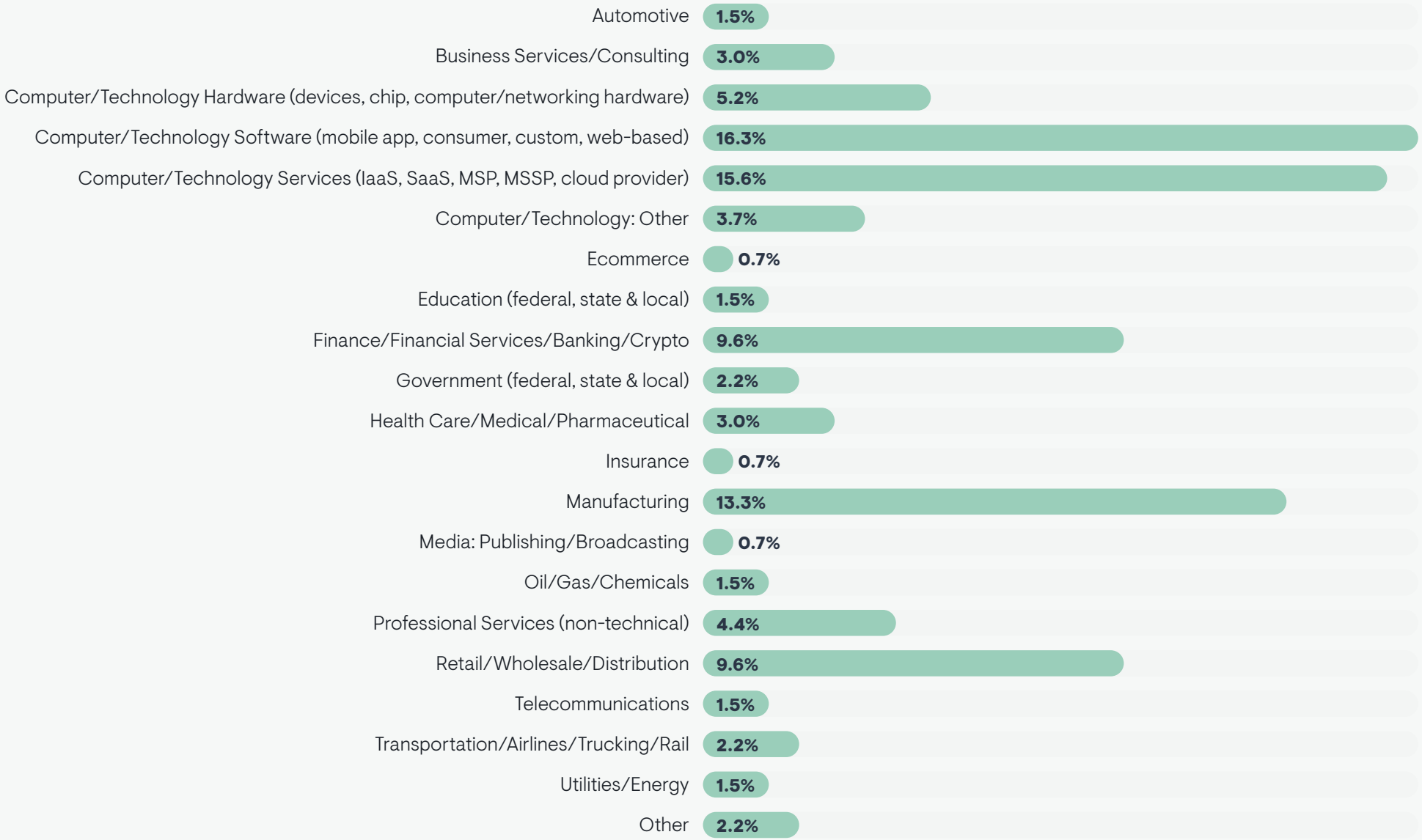
Omada's platform uses AI-driven insights and intelligent automation to enforce just-in-time, least-privilege access. With unified visibility and continuous risk evaluation, Omada enables security teams to detect threats faster, strengthen control, and scale identity security without added complexity.

# Demographics

**In total, how many employees are currently working in your organization?**



**Which of the following best describes your organization's primary industry?**



## About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT research and consulting firm dedicated to delivering actionable insights across the evolving technology landscape. Through independent research, market analysis, and vendor evaluations, we empower organizations to make well-informed technology decisions. Our team of analysts combines practical experience with a deep understanding of industry best practices and emerging vendor solutions to help clients achieve their strategic objectives. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.



2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4661.012026