DIGITAL IDENTITY SURVEY 2025

23 February 2026

Table of contents

Platform voor InformatieBeveiliging

Conclusions & Insights

PvIB

Platform voor
InformatieBeveiliging

Overall Conclusions & Insights

Introduction

The Digital Identity Survey 2025 provides a detailed look at how organizations currently manage Identity and Access Management (IAM). By combining structured data with direct professional insights, the survey highlights a landscape where IAM is recognized as a foundational capability for security and digital operations.

This survey explores the current state of IAM across various industries, focusing on the strategic goals, technological shifts, and operational hurdles that organizations face today. The results reflect the real-world experiences of professionals managing complex identity ecosystems in a rapidly evolving digital environment.

The following sections detail the specific findings across the main pillars of the survey.

Value Drivers

Organizations pursue several goals with their IAM activities. While security remains the primary driver, there is an increasing push for business enablement.

Security and Governance: Organizations primarily use IAM to protect themselves. Across all industries, cybersecurity, governance, compliance, and internal control remain the absolute top priorities. This highlights that IAM is still seen as a foundational risk management capability and a primary defense mechanism.

Business Enablement: Beyond security, organizations expect IAM to drive an optimized user experience and productivity among target user groups like their customer, workforce and business partners. It must facilitate remote and hybrid work and streamline the identity lifecycle and support processes for end-users; however, fragmented environments often lead to a mixed user experience, suggesting that IAM is more mature as a security control than as a business facilitator.

IAM Trends

Several key developments are currently shaping the future of the IAM landscape:

Identity-Centric Security: As organizations move toward cloud platforms and SaaS, Zero Trust principles are being put into practice. Access is no longer granted based on network location, but on the verified identity of the user.

Identity Federation: There is a clear trend toward adopting federation models that empower diverse user groups to securely access the digital landscape, shifting away from isolated identity silos toward an interconnected ecosystem.

Authentication: Modern methods, such as passwordless authentication and MFA, are key to IAM modernization. While these methods improve security and usability, they often coexist with the legacy approach of using passwords. As a result, the application of modern authentication remains uneven across different systems and user groups.

Non-Human Identities: There is growing recognition that IAM must also address non-human identities, such as service accounts and automated processes. While these are part of future roadmaps, governance practices for them are not yet consistently defined. This indicates an expanding IAM scope that is still needs maturing.

Access Control Models: There is a notable shift in interest toward dynamic and context-aware authorization models; however, Role-Based Access Control (RBAC) remains the dominant standard in practice due to its inherent predictability and suitability for audit requirements.

Emerging Technologies: Technologies like AI-driven IAM and decentralized identity are acknowledged as impactful but are currently rarely implemented at scale. Most organizations focus on stabilizing their core IAM capabilities before adopting emerging tools.

Overall Conclusions & Insights (2)

IAM Adoption and Use

This section examines the current state of IAM development and how implementation methods vary across different sectors.

IAM Solutions: In regulated industries like Financial Services, Public Sector, Healthcare, and Energy, investments are driven by security, privacy, and audit requirements. In other industries like Manufacturing, Retail, and IT & Services, the focus shifts more toward automation and efficiency within complex legacy setups.

Operational Baseline: Most organizations have established a baseline that includes SSO, MFA, and automated provisioning. However, the depth varies: regulated industries focus more on formal access reviews, while the other industries prioritize federation and user onboarding flows.

Adoption constraints: Maturity is often limited by practical factors such as cost, ROI justifications, and dependencies on specific vendors, leading to pragmatic rather than "ideal" setups.

Implementation Challenges

The most significant hurdles to successful IAM programs are often organizational or data-related rather than purely technical.

IAM Governance: Challenges arise from ownership being split across business, IT, architecture, and security functions. A lack of alignment among different stakeholders regarding responsibilities and approvals slows down decision-making and undermines consistent enforcement.

IAM Integration: Connecting IAM to a mix of cloud, SaaS, and on-premises legacy systems is the top execution challenge. Hybrid and multi-entity environments significantly increase the effort required for technical integration, while partner and third-party access flows often involve longer approval chains and weaker attestation coverage.

Role Design: Designing and maintaining roles and permission structures at scale is a major source of friction. Role-Based Access Control (RBAC) remains dominant because it is predictable and auditable. Advanced policy- or attribute-based approaches are introduced selectively, resulting in incremental rather than transformative change.

Data Quality: Fragmented identity data and a lack of authoritative sources remain limiting factors for automation. Without a "single source of truth," processes like provisioning remain manual and inefficient, even when modern IAM tools are available.

IAM Transition: Every IAM journey is unique, shaped by the specific context in which an organization operates. Factors like the scale of the organization, budget, and available internal skills directly determine the pace and success of the transition.

Introduction

Platform voor
InformatieBeveiliging

Digital Identity survey 2025

Digital Identities or Identity and Access Management (IAM) are a vital part of modern security and digital operations. As organizations move to the cloud and face more cyber threats, IAM has become a central tool for managing risk and maintaining control.

To address this in more detail, the PvIB launched a Special Interest Group (SIG) for IAM in 2024. The group's goal is to share knowledge and practical experience, while identifying common challenges and best practices within the professional community.

To address this, PvIB conducted a survey among its members to understand how IAM is implemented and managed in practice. The survey focuses on real-world experiences, covering technical requirements, current technologies, emerging trends, and operational challenges. It captures insights from a broad range of professionals, including practitioners as well as those in oversight, security, and risk management roles.

Protiviti, a global consulting firm specialized in risk management and information security, analyzed these results, which are presented in this report. The goal of the report is to provide a clear overview of current IAM practices, highlight what makes them successful, and point out where the difficulties lie. It is intended to serve as a reference for discussion and knowledge sharing, rather than as a formal benchmark or a maturity assessment.

Based on your input, this report offers an overview of current Identity & Access Management practices, future trends and challenges.

Survey Respondents

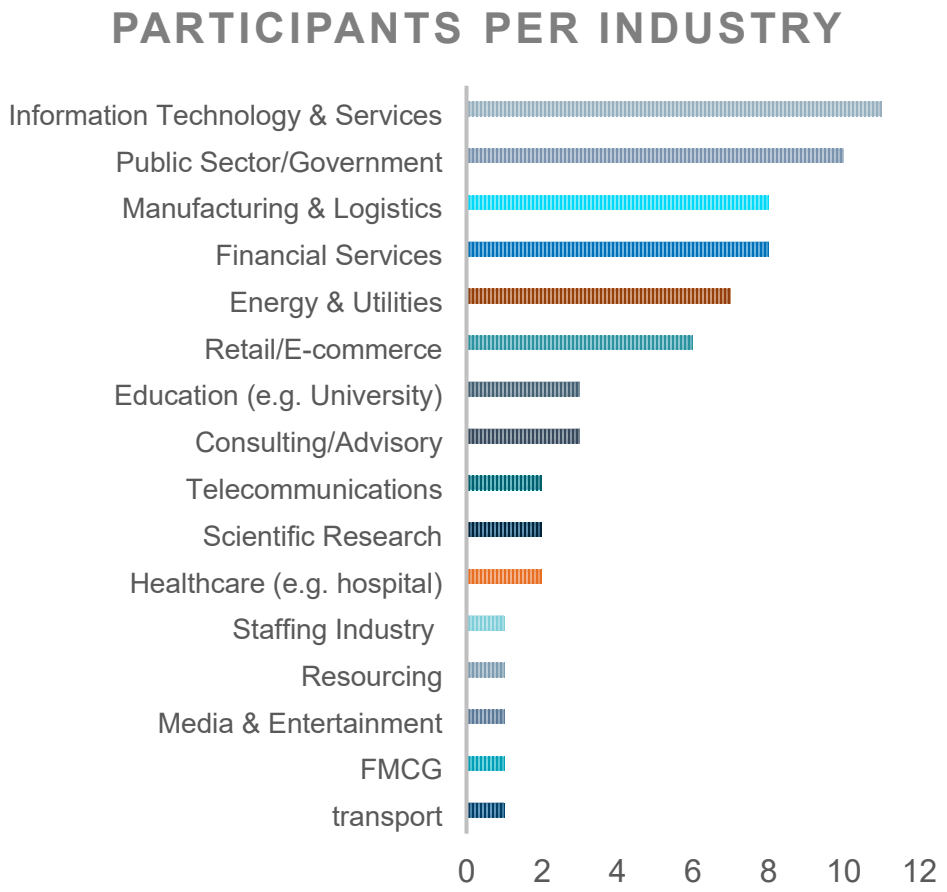
The survey is based on responses from 67 participants representing a variety of organizations, industries, roles, and IAM environments. Many respondents hold senior positions, including Risk Managers (42%) and Product Owners (27%), which indicates that the responses are backed by responsibilities related to risk, governance, oversight, and solution ownership.

Respondents span a broad cross-section of industries, as outlined in the chart to the right. Participants come primarily from mid-sized to large organizations, ranging from single legal entities to multi-entity group structures operating at both national and international levels. This reflects a diverse mix of organizational models and operating scopes.

The IAM environments covered in the survey vary significantly in scale, from organizations managing relatively small identity populations to those supporting large-scale enterprise environments. These differences highlight varying levels of operational scope, regulatory requirements, and organizational complexity across the group.

For many respondents, IAM is primarily focused on the workforce. However, about one-third reported that their IAM scope also covers customer identities (CIAM), showing that customer requirements are a meaningful priority for a significant subset of participants.

Taken together, this respondent profile provides a good look into IAM practices across different industries, structures, scales, and roles, based on input from individuals with direct, relevant responsibilities.



Survey Results

Platform voor
InformatieBeveiliging

Value drivers of IAM

The survey results show that organizations mainly value IAM as a capability for security and governance. Participants indicate that cyber security, compliance, and internal control are very important. This makes IAM an essential foundation for managing risks, meeting legal requirements, and strengthening trust within the organization.

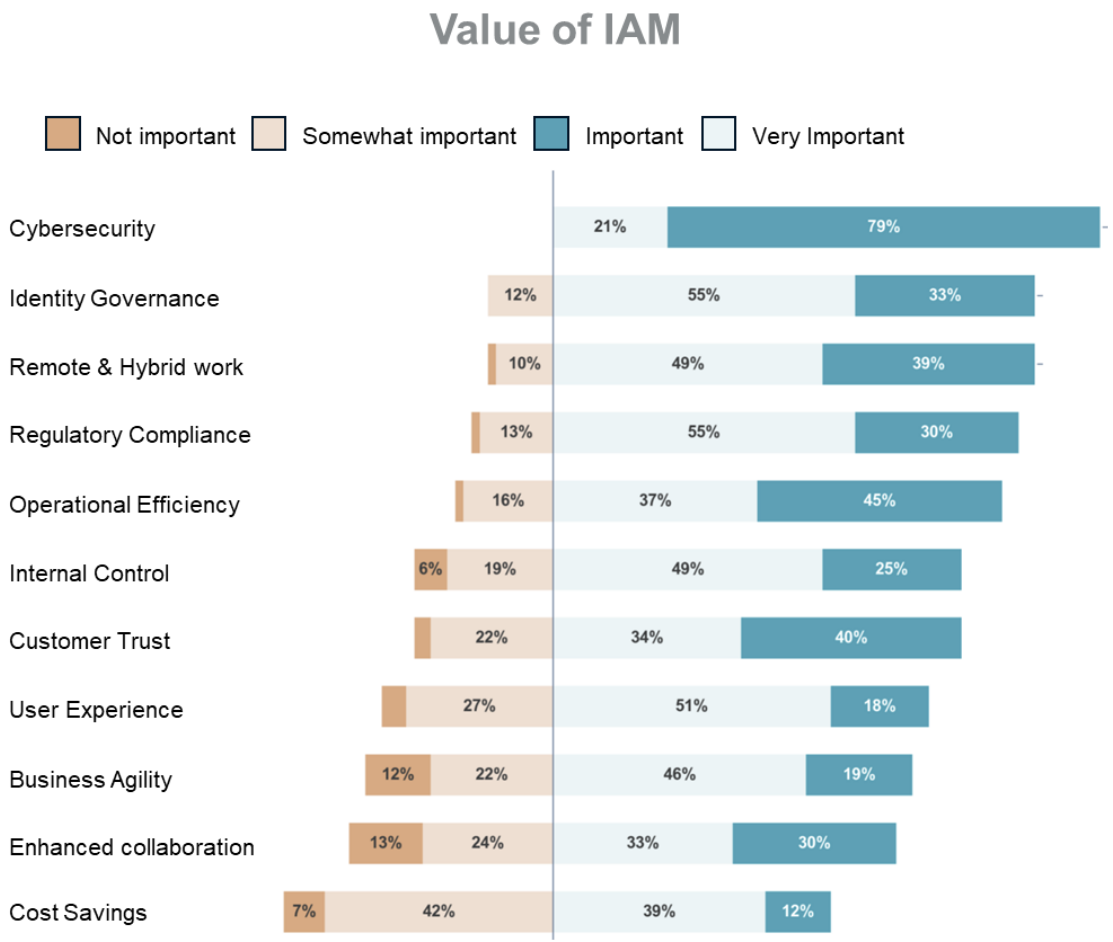
At the same time, participants link IAM to business benefits. They mention things like operational efficiency, support for hybrid work, and a better experience for users. This shows that IAM is seen as both a control mechanism and a tool that helps the business move forward, depending on how mature the organization is in this area.

Several participants make a direct link between IAM and faster access delivery, central management, and the ability to adapt to changes in the workforce. IAM is also mentioned in the context of innovation; for example, it helps organizations move to the cloud more easily or implement other major changes.

New regulations, such as NIS2, ensure that there is more focus on IAM and that improvements are carried out faster. IAM is widely seen as necessary and valuable. It is crucial for stopping unauthorized access, protecting sensitive data, and ensuring that audits run smoothly.

When asked what is still missing, most people indicated that the current topics represent their priorities well. Where additions were mentioned, they mainly concerned data privacy, standardization, digital sovereignty, and access for customers or partners.

Finally, opinions are divided on whether IAM actually delivers what it promises at this moment. Although everyone sees the value for security and compliance, this is not always achieved in practice. Fragmented tools, systems that do not cover everything, outdated technology, and manual processes lead to mixed results. Because of this, benefits such as scalability, self-service, and a good user experience are not yet realized everywhere.



Current IAM trends

Respondents see the Zero Trust Security Model and cloud computing as the main trends shaping the future of IAM. This shows a clear focus on security that centers on identity to support spread-out, cloud-based environments and modern apps.

Respondents see the Zero Trust Model and cloud computing as the main trends shaping the future of IAM. This shows a clear focus on identity-centric security architecture to support hybrid technology environments and modern applications.

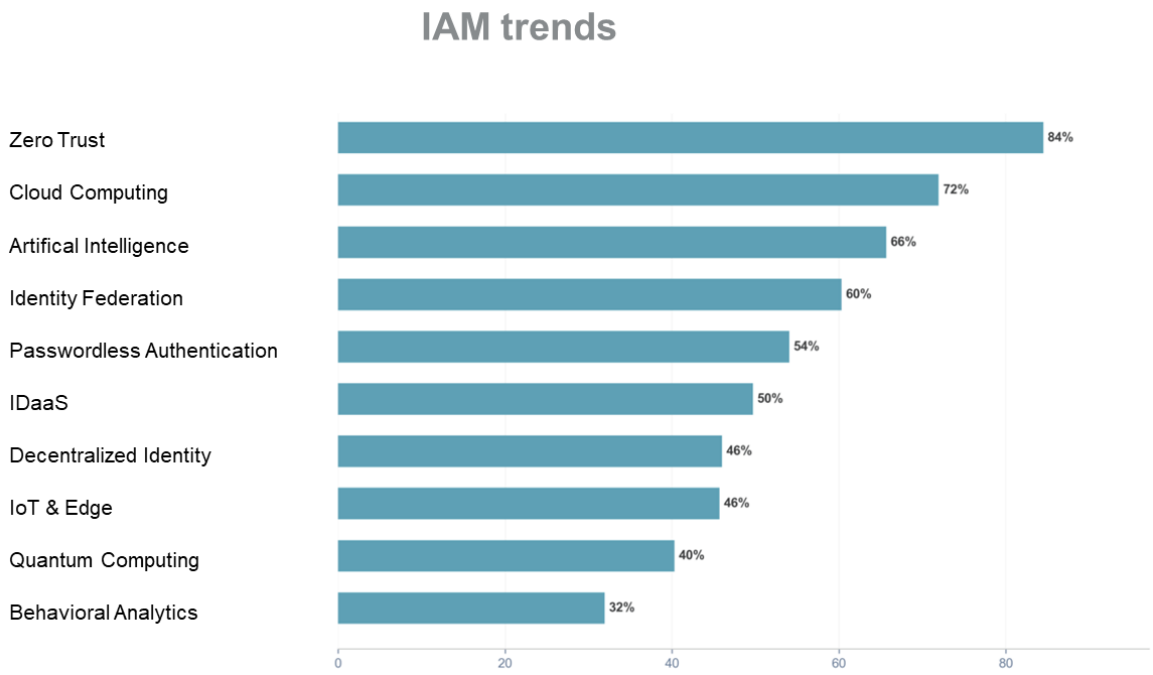
Identity federation and artificial intelligence are also seen as relevant trends. Respondents consistently describe identity federation as a practical and established capability that allows access across different applications. AI and machine learning are recognized as important, but respondents rarely give specific examples of how to use them for IAM right now, making them feel more like future goals.

Passwordless login and Identity as a Service (IDaaS) are central parts of the trend overview. Respondents see these as ways to modernize IAM, especially for moving to the cloud, making login simpler, and reducing daily complexity. At the same time, they note that these new methods often must work alongside old systems, which leads to a mix of different standards across the organization.

Decentralized identity (self-sovereign identity) is still a lower-ranked trend and is mostly discussed for specific new uses, like digital wallets, rather than as a widely used IAM capability. Quantum computing is ranked near the bottom and is described as a long-term topic rather than a current priority. Behavioral analytics and detection tools are also ranked low and are not seen as a priority by respondents.

Overall, respondents describe a clear group of trends that show where IAM is going: Zero Trust, cloud-based IAM, federation, modern login models, a wider scope of identities, and more detailed ways to grant access.

In the open responses, respondents also mention non-human or machine identities and the further development of policy-based and attribute-based access models (PBAC/ABAC) as areas to watch.



IAM Adoption and use

IAM solutions in place

Organizations operate IAM landscapes consisting of multiple solutions that address identity, access, and governance. The survey results indicate differences in which solutions are implemented and the extent of their application across organizations.

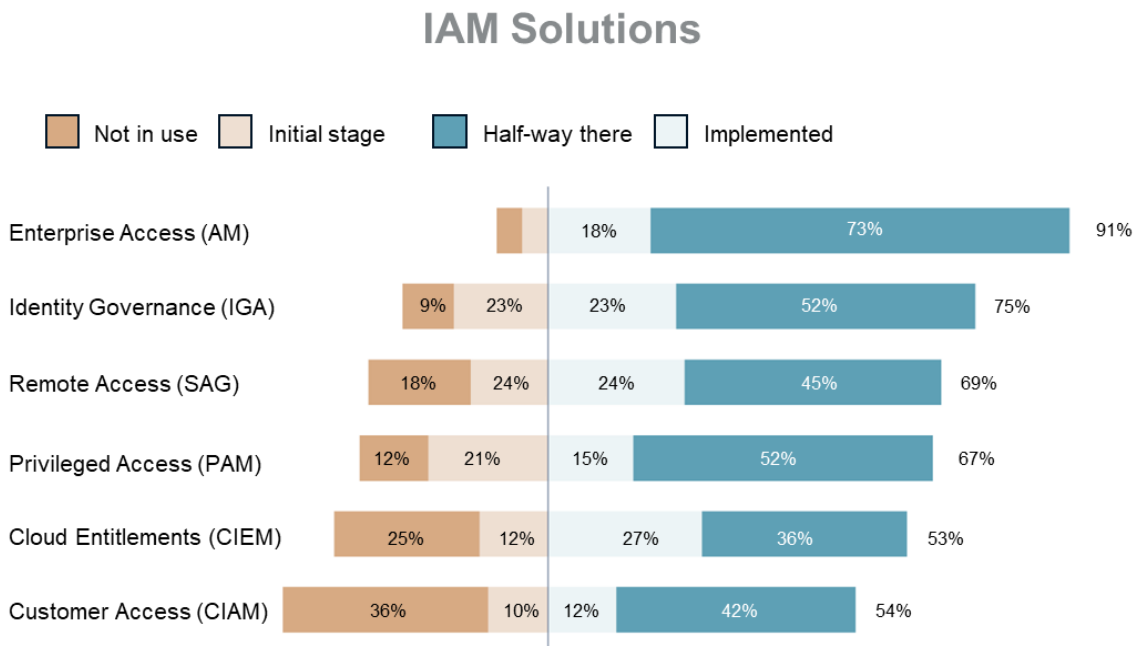
Access Management (AM) solutions and directory services are widely in use. These are delivered through on-premises platforms or cloud-based Identity as a Service (IDaaS) offerings. The solutions provide authentication, access enforcement, and federation across IT environments and applications.

The adoption of Identity Governance and Administration (IGA) varies across industries. Some IAM landscapes include dedicated governance solutions, while others use limited or no governance-specific tooling. This results in variations in identity governance capabilities. These differences are observed when comparing regulated industries, where governance- and control-oriented solutions are present, to IAM landscapes in other sectors.

Privileged Access Management (PAM) solutions exist as a component within many IAM landscapes. PAM is implemented alongside other IAM solutions and is used to control access to privileged or high-risk accounts.

In environments with external user populations, Customer Identity and Access Management (CIAM) solutions are present. This indicates an expansion of IAM scope beyond workforce identities. The data does not provide a basis for conclusions regarding how CIAM is architecturally positioned relative to workforce IAM.

Open responses provide additional context. Respondents describe IAM landscapes as being influenced by legacy systems and the incremental adoption of new solutions. Several respondents indicate uneven coverage of governance-oriented solutions and challenges related to system integration. In scenarios involving external users, respondents refer to onboarding, user journeys, and consistency as areas requiring attention.



IAM Adoption and use

IAM Procurement drivers

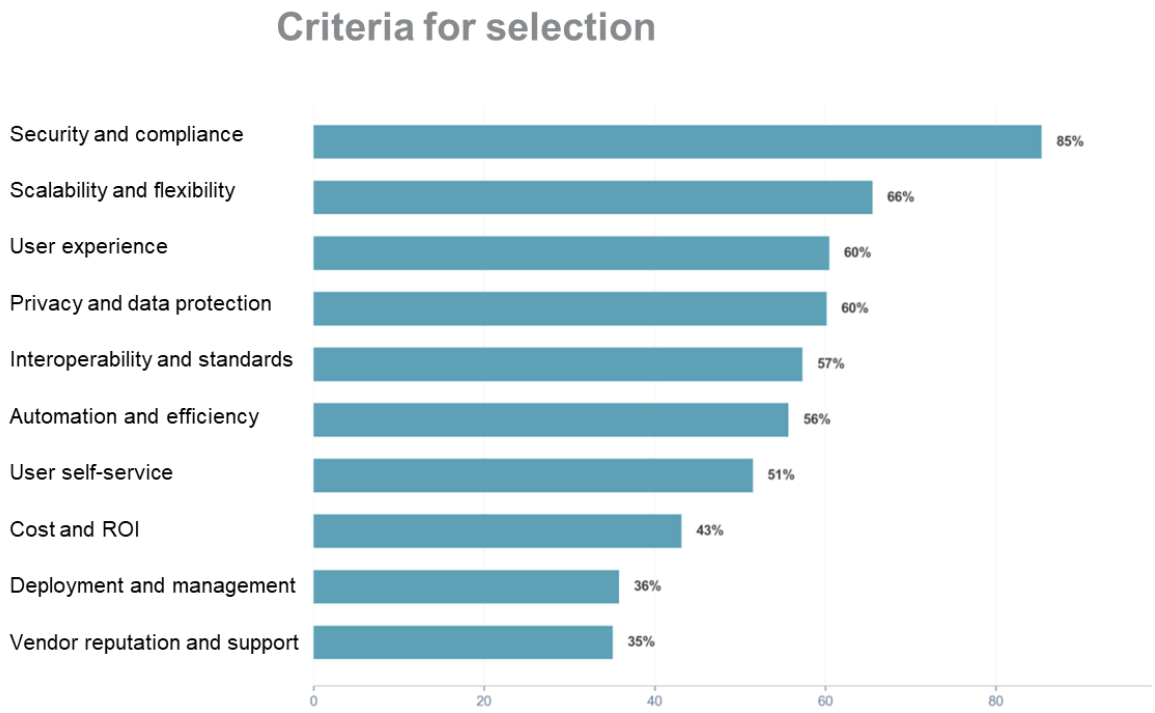
The purchase of IAM solutions is mainly driven by security and compliance. Organizations focus on privacy and data protection rules. In regulated sectors like finance, energy, healthcare, and the public sector, audit requirements and regulatory pressure are important reasons for investing in IAM. Open remarks show that regulatory rules and risk management act as the primary accelerators for these projects.

At the same time, organizations in all industries look for better automation, efficiency, and scalability. In large environments—such as manufacturing, retail, and multinational companies—IAM is bought to manage many identities and reduce manual work. It also helps organizations handle complex and legacy systems. Open responses mention that replacing old or custom-built solutions with standardized new IAM tools is a major goal.

User experience is valued differently depending on the sector. In education, professional services, and retail, the focus is on user-friendly self-service capabilities. In high-security sectors, usability is often a secondary goal, though it is becoming more important. Open remarks show a shift where IAM is expected to provide both control and a smooth user journey with easy access.

Finally, practical factors influence the scope and speed of procurement. These include how well new solutions work with existing applications, the effort needed for management, and the total cost. Several remarks note that it can be difficult to build a business case when the benefits are hard to measure or when the technical complexity is high.

In summary, IAM procurement is a balance between meeting regulations, making operations manageable, and meeting higher expectations for usability and business value.



IAM Adoption and use

IAM methods in use

The survey shows that IAM methods vary in scope and automation levels. This provides a view of how IAM solutions are used in daily operations.

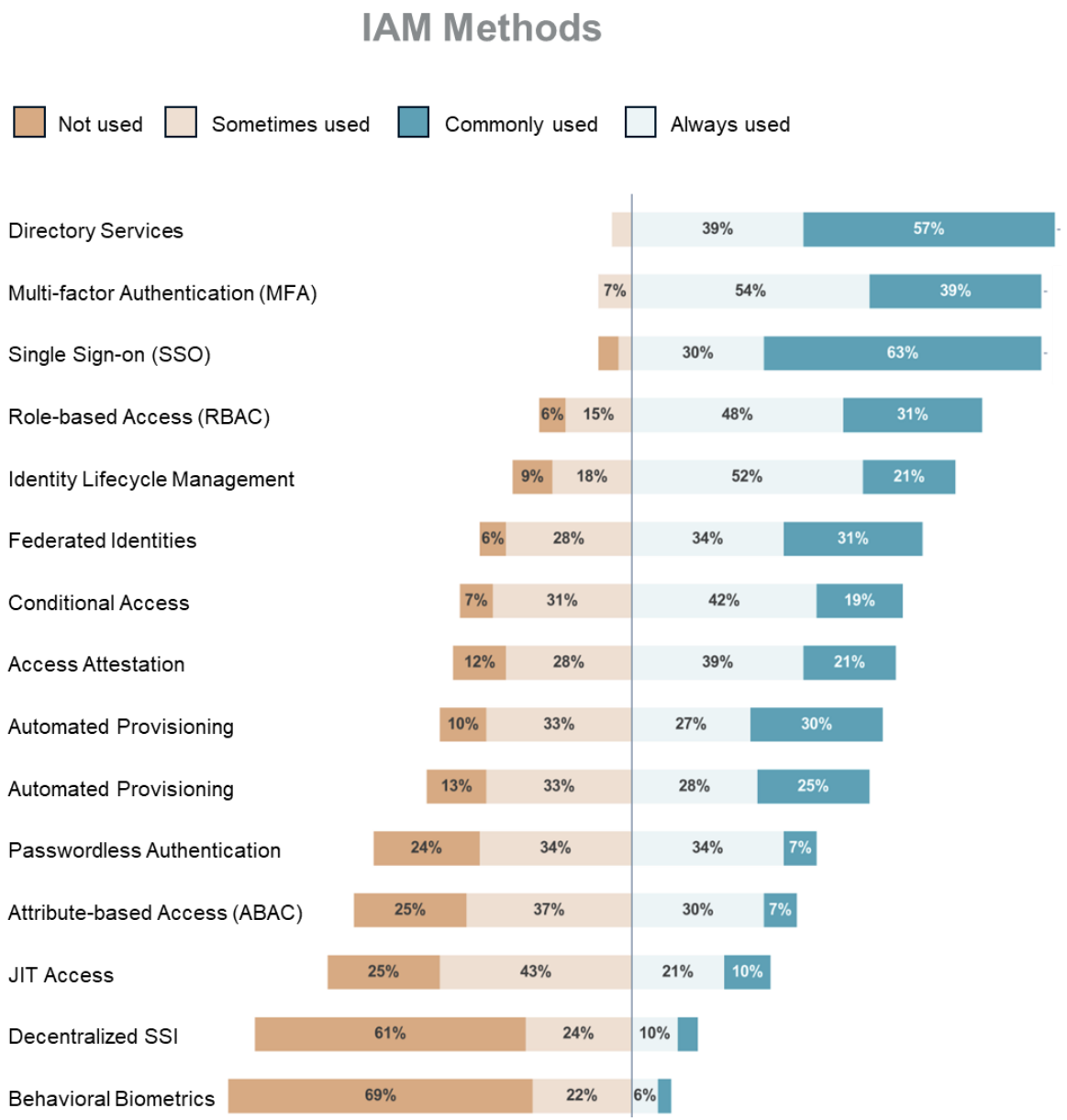
Respondents indicate widespread use of authentication methods, including Single Sign-On (SSO) and Multi-Factor Authentication (MFA). These methods support access across multiple applications and environments. Advanced access methods, such as conditional access and Just-in-Time (JIT) access, are used in some environments but are not adopted by all organizations.

Identity lifecycle management and automated provisioning are very common. At the same time, there is variation in consistency and coverage. This points to differences in how broadly these methods are applied.

The use of authorization methods varies across environments. Role-Based Access Control (RBAC) is used broadly. Attribute-Based Access Control (ABAC) and policy-driven authorization are used less often. This reflects differences in how authorization models are designed and applied.

Across industries, authentication, identity lifecycle management, and automated provisioning form a common baseline. The industry context influences how other methods are applied. Regulated environments focus more on access reviews and authorization controls. In contrast, organizations with large or diverse user populations place more emphasis on federation and onboarding.

Open responses provide more context. Respondents mention manual steps in IAM processes, problems with connecting to legacy systems, and complexity in decentralized environments. Where external users or multiple identity populations are involved, respondents mention onboarding and consistent user journeys as areas that need attention.



IAM Implementation challenges

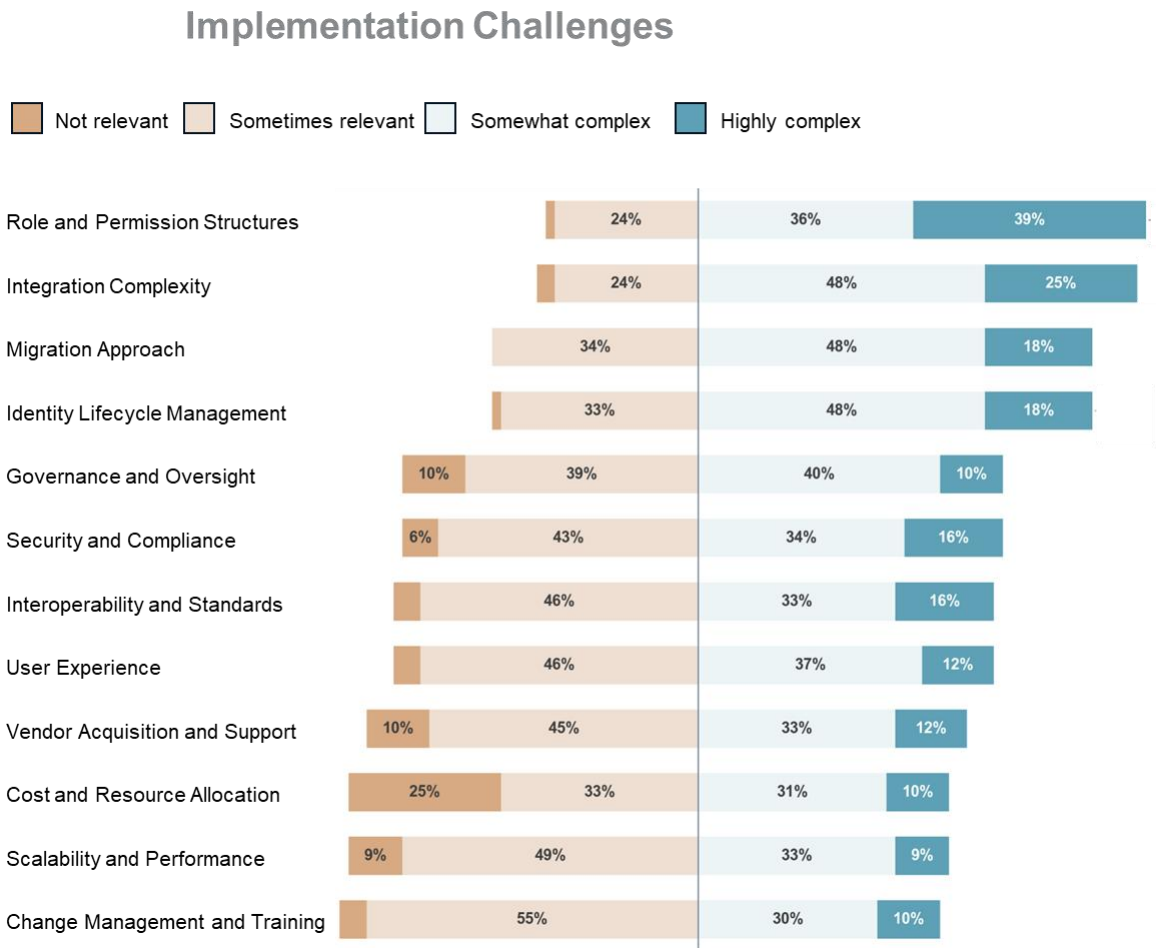
The survey results show that IAM implementation challenges are mostly linked to governance and oversight, role and permission structures, integration complexity, and security and compliance. These are identified as the most demanding parts of an IAM implementation. This reflects the difficulty of applying controls and structures consistently across different systems and organizations.

Governance and role definition are highlighted as the most demanding areas. Establishing and maintaining a clear framework for roles across evolving application landscapes is a persistent and resource-intensive challenge. Security and compliance also remain central, as it takes significant effort to meet regulatory and audit requirements consistently in complex, heterogeneous environments.

Other challenge areas are also mentioned, though their importance depends more on the specific project and scope. These include user identity lifecycle management, interoperability and standards, and the migration approach. Respondents also point to user experience, vendor acquisition and support, cost and resource allocation, scalability and performance, and change management and training.

The industry context shows that while the challenges are similar, the emphasis differs. Public Sector and Financial Services focus more on governance, security, and roles. Manufacturing, Logistics, and Energy & Utilities place more emphasis on integration, interoperability, and scalability. Retail, e-commerce, and Education/Research more frequently point to migration and user experience, often alongside change management and training.

Open responses provide more context by referring to legacy systems and fragmented application landscapes. They also highlight the difficulty of uneven role models, manual steps and exceptions, and dependencies on resources or vendors. These remarks indicate that challenges come less from missing IAM solutions and more from the complexity of applying them consistently and at scale within a specific organizational context.



Appendices

Substantiation

A short explanation on the methods of analysis

Introduction to the results

The results are presented in two layers. Structured questions provide a quantitative view on IAM value drivers, trends, solution adoption, and implementation challenges, while open-text responses add qualitative context on how these are experienced in practice. Together, they offer insight into both IAM maturity and the factors driving or hindering adoption.

Results are analyzed by industry and respondent role, highlighting sector-specific priorities and differences in perspective across operational, managerial, and executive levels. This combined view reveals where industries align or diverge and identifies the key cross-cutting barriers to maturity.

How the data was analyzed

The survey combined structured questions (Likert-scale items, multi-select, and ranking exercises) with open-text responses. Structured data were analyzed using descriptive statistics to identify overall patterns and key trends.

Open-text responses were reviewed and grouped into recurring themes, providing qualitative context to the quantitative findings.

Together, these approaches provide a cross-sectional view of IAM priorities, adoption, and challenges across industries and respondent roles, highlighting both what organizations prioritize and how these are experienced in practice.

About the authors

Evert van Zanten
Programmamanager
Cyber Security
Trusted Advisor IAM
Voorzitter PvIB
Kwartiermaker PvIB SIG-IAM

Evert van Zanten has a background in Information Security & Privacy, with a specialization in Identity & Access Management.. He is involved in the Cyber Security Alliance and the Online Trust Coalition. He and a board member of PvIB since 2019. He is its chairman since April 2026.

He led IAM initiatives at UWV, European Central Bank, and acts as a Trusted Advisor for Randstad Global and the Municipality of Arnhem.

Protiviti
Marcel Koers
Technology Consulting
SME Cyber Security & IAM
Qualified Auditor (RE)

Marcel Koers is a Information Security & Privacy specialist with IT Audit background. He has audited, advised and implemented IAM for several organizations over the years.

He co-developed the 2025 IAM survey together with PvIB and was involved in shaping the report.

Protiviti
Paul Taalman
Technology Consulting
SME Cyber Security & IAM
Qualified Auditor (RE)

Paul Taalman works as a Cybersecurity specialist and IT Auditor at Protiviti. He has extensive experience in audit, IT risk management, and cybersecurity. He supports organizations in designing, assessing, and controlling digital identity and access processes.

He co-developed the 2025 IAM survey together with PvIB and was involved in shaping the report.

Platform voor Informatiebeveiliging

PvIB (Platform voor Informatiebeveiliging) is the Dutch professional association for information security practitioners. Through knowledge sharing, publications, working groups, and community events, PvIB connects security professionals and contributes to advancing the practice of information security — including on topics such as digital identities, cyber resilience, and regulatory developments like NIS2.

Protiviti

Protiviti is a global business consulting firm delivering expertise across risk, compliance, technology, and digital transformation. Protiviti the Netherlands practice is based in Amsterdam and serves clients ranging from large corporates to public sector organizations across a wide range of industries.

With more than 11,000 professionals in 25 countries, Protiviti combines global reach with local insight to help organizations navigate an increasingly complex regulatory landscape. Protiviti provides specialized cybersecurity consulting — including strategy, risk assessments, and regulatory compliance — as well as Identity and Access Management (IAM) services that help organizations design, implement, and govern the controls needed to protect critical systems and meet obligations such as those imposed by NIS2.