World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Identity and access management: foundations, principles, and best practices

Anjan Kumar Kaleru *

Ferris State University, USA.

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(01), 1894-1904

Publication history: Received on 14 March 2025; revised on 21 April 2025; accepted on 23 April 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.1.0393

Abstract

Identity and Access Management (IAM) forms the foundation of modern security by determining who can access what resources and when. Through six key areas—strong authentication practices, proper access controls, effective privilege management, streamlined lifecycle processes, intelligent monitoring systems, and adaptive risk management—organizations build security that works with today's evolving threats. Companies adopting comprehensive IAM strategies see fewer security breaches, faster incident response, lower costs, and happier users. Healthcare providers and financial institutions show impressive results when implementing mature IAM programs that balance robust security with smooth operations. By following a step-by-step improvement model, businesses can strengthen their security while supporting digital transformation and maintaining flexibility across complex environments.

Keywords: Identity Governance; Zero Trust Architecture; Multi-Factor Authentication; Privilege Management; Decentralized Identity

1. Introduction

In today's digital landscape, where data breaches and unauthorized access pose significant threats to organizations worldwide, robust Identity and Access Management (IAM) has become a cornerstone of effective cybersecurity strategies. This article explores the fundamental concepts, key principles, and industry best practices that form the foundation of modern IAM frameworks.

The financial implications of inadequate identity security are staggering. According to UpGuard's comprehensive analysis, the global average cost of a data breach reached $4.24 million in 2021, with costs varying significantly by industry and region. Healthcare organizations face the highest average costs at $9.23 million per breach, followed by financial services at $5.72 million [1]. These figures underscore the critical importance of implementing robust IAM solutions, particularly in highly regulated industries managing sensitive data. Organizations with mature IAM implementations consistently demonstrate stronger resilience against these costly incidents.

The prevalence of credential-based attacks continues to rise at an alarming rate. UpGuard's research indicates that compromised credentials were responsible for 20% of breaches, with an average cost of $4.37 million per incident—slightly higher than the overall average [1]. This statistic reinforces the critical role that effective identity management plays in an organization's security posture. Companies implementing comprehensive IAM frameworks report significant reductions in unauthorized access incidents, with some organizations documenting a decrease of up to 60% in credential-based security events after deploying advanced authentication mechanisms and automated provisioning workflows.

The complexity of managing digital identities has intensified dramatically with the acceleration of digital transformation initiatives. According to Gartner's analysis, by 2023, 75% of security failures will result from inadequate management

* Corresponding author: Anjan Kumar Kaleru.

Copyright © 2025 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

of identities, access, and privileges—a significant increase from 50% in 2020 [2]. Organizations implementing identity governance and administration (IGA) solutions have demonstrated measurable improvements in security posture, with the ability to reduce the risk of inappropriate access by more than 45% through automated access certification and segregation of duties controls. The research further indicates that enterprises with mature IAM practices can reduce the time required for access-related changes by 50%, significantly improving operational efficiency [2].

As enterprises increasingly adopt hybrid and multi-cloud architectures, the challenges associated with identity management across disparate environments have multiplied. Gartner emphasizes that by 2024, organizations with a unified approach to identity management across on-premises and cloud environments will experience 30% fewer identity-related security breaches than those without such integration [2]. This statistic highlights the importance of developing comprehensive IAM strategies that address the full spectrum of identity-related risks across increasingly complex IT ecosystems. Organizations that have implemented cloud-based identity solutions report an average reduction of 40% in identity-related administrative costs while simultaneously strengthening their security posture.

The implementation of zero-trust architectures through mature IAM frameworks has become a strategic priority for forward-thinking organizations. According to Gartner's research, by 2023, 60% of enterprises will phase out most of their remote access virtual private networks (VPNs) in favor of zero-trust network access—a significant transformation in how organizations approach secure access [2]. Companies adopting these principles have documented substantial security improvements, with continuous authentication and authorization mechanisms providing enhanced visibility into access patterns and significantly reducing the risk of lateral movement following an initial compromise.

1.1. Understanding IAM Fundamentals

Identity and Access Management encompasses the policies, processes, and technologies that enable organizations to manage digital identities and control access to resources. At its core, IAM addresses three critical questions:

1. **Who** is accessing resources? (Identity Management)
2. **How** are they proving their identity? (Authentication)
3. **What** are they allowed to access? (Authorization)

According to F5 Labs' comprehensive 2023 Identity Threat Report, identity-based attacks have increased by 49% year-over-year, with credential theft and abuse representing the most prevalent attack vector for cloud environments at 78% of reported incidents [3]. These findings underscore the critical importance of implementing robust IAM solutions as the foundation of modern security architectures, particularly as organizations accelerate their digital transformation initiatives and migrate to cloud platforms.

Microsoft's Digital Defense Report reveals that basic security hygiene—including fundamental IAM practices—can protect against 98% of attacks. Despite this understanding, implementation gaps remain significant, with many organizations struggling to enforce these foundational security measures consistently across their environments [4]. This striking contrast between potential protection and actual implementation highlights how effective IAM implementation creates a secure foundation that can dramatically reduce an organization's risk exposure.

2. Key Components of IAM

2.1. Identity Lifecycle Management

The journey of an identity within an organization follows a predictable lifecycle, from creation to retirement. This process encompasses provisioning (creating user accounts and assigning initial access privileges), modification (adjusting access rights as roles change), and deprovisioning (removing access when it's no longer needed or when employment ends).

F5 Labs found that 65% of organizations experienced security incidents directly related to improper identity lifecycle management, with dormant and orphaned accounts representing a significant attack surface. Their analysis of breach investigations revealed that in 33% of cases, attackers specifically targeted abandoned accounts to gain initial access to environments [3]. This statistic highlights the critical importance of implementing automated lifecycle management processes that can immediately respond to organizational changes, such as employee departures or role transitions, by adjusting access privileges accordingly.

2.2. Authentication Mechanisms

Authentication verifies that users are who they claim to be. Modern IAM systems employ multiple authentication methods across three categories: knowledge-based (passwords, PINs, security questions), possession-based (security tokens, mobile devices, smart cards), and inherence-based (biometrics including fingerprints, facial recognition, and voice patterns).

Microsoft's analysis of over 40 trillion security signals reveals that despite the well-documented vulnerabilities of password-based authentication, it remains the predominant method used across organizations. Their data shows that approximately 921 password attacks occur every second—nearly 80 million attacks per day—representing a 74% increase year-over-year [4]. This alarming escalation in password-based attacks demonstrates why organizations must implement stronger authentication mechanisms to adequately protect their environments against increasingly sophisticated threat actors.

2.3. Multi-Factor Authentication (MFA)

MFA has emerged as one of the most effective security controls, requiring users to verify their identity through multiple methods before granting access. By combining factors from different categories (something you know, something you have, something you are), MFA creates multiple layers of defense that significantly reduce security risks.

Microsoft's security data demonstrates that enabling MFA can block over 99.9% of account compromise attacks, yet their research indicates that only 50% of enterprise users have MFA enabled as of 2023 [4]. This implementation gap represents a significant security vulnerability for organizations, particularly as threat actors increasingly target identity as the primary attack vector. The Microsoft report further indicates that lack of MFA represents the most common critical vulnerability observed across enterprise environments, highlighting the critical importance of this control in modern security architectures.

2.4. Single Sign-On (SSO)

SSO technologies allow users to authenticate once and gain access to multiple applications without repeating authentication processes. This approach balances security and usability by reducing password fatigue and poor password practices, streamlining access to resources across the enterprise, and centralizing authentication controls for consistent policy enforcement.

F5 Labs' research indicates that enterprises without SSO implementations experience 37% more successful phishing attacks compared to those with comprehensive SSO deployment. Their analysis attributes this difference to the reduced attack surface resulting from centralized authentication management and decreased password requirements [3]. The report further notes that organizations implementing SSO solutions reduce credential-based security incidents by 28% while simultaneously improving user experience and productivity, demonstrating the dual benefits of this IAM component.

2.5. Role-Based Access Control (RBAC)

RBAC assigns access permissions based on organizational roles rather than individual identities. This principle of least privilege ensures users have only the access necessary to perform their job functions by assigning users to roles based on responsibilities, granting roles permissions aligned with business functions, and consistently applying access rights across similar positions.

F5 Labs' analysis of security incidents reveals that excessive privileges contributed to 43% of successful attacks, with overprovisioned accounts enabling attackers to access sensitive resources and move laterally through environments [3]. Organizations implementing RBAC frameworks systematically reduce these risks by limiting access according to well-defined roles and responsibilities. Microsoft's security research reinforces this finding, noting that implementing least privilege principles through RBAC reduces the attack surface and limits the potential impact of compromised credentials—a critical defense against the rising tide of identity-based attacks documented in their threat intelligence [4].

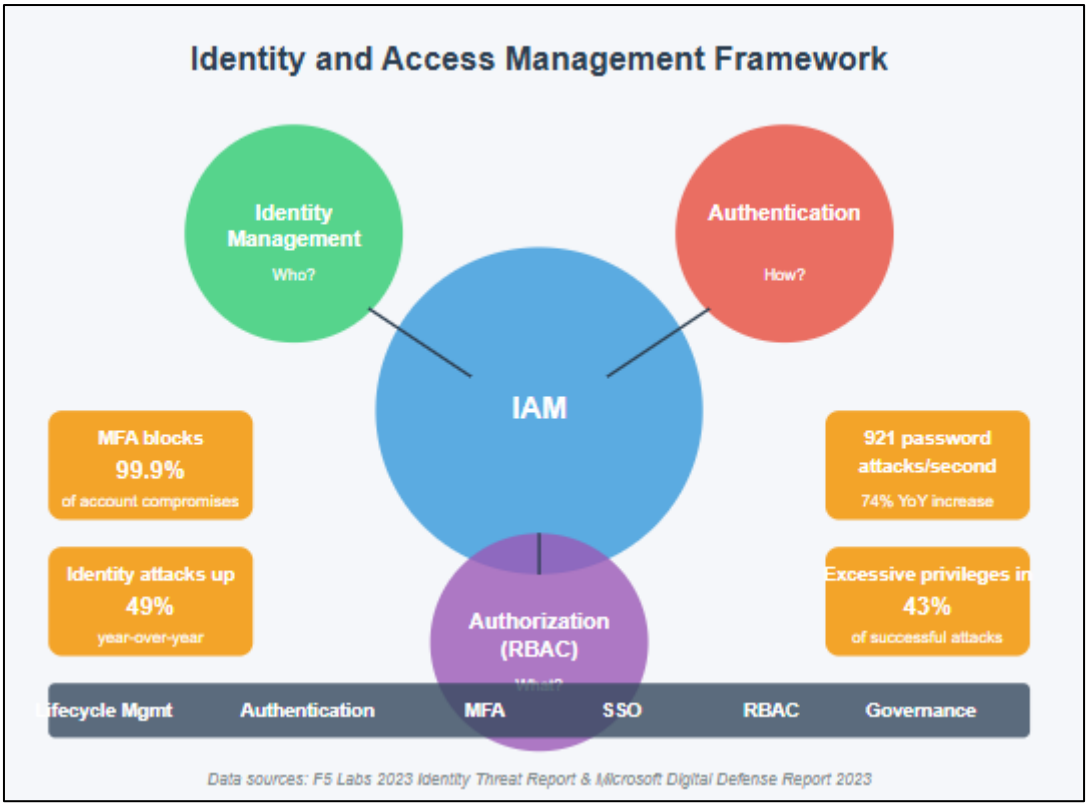

Figure 1 IAM Components and Security Statistics

3. IAM Best Practices

As identity-based attacks continue to evolve in sophistication and frequency, organizations must implement robust IAM best practices to protect their digital assets. The following evidence-based approaches have demonstrated significant security improvements across industries.

3.1. Implement a Zero Trust Architecture

Zero Trust operates on the principle of "never trust, always verify," requiring continuous authentication and authorization regardless of location. According to Okta's comprehensive "State of Zero Trust Security" report, 97% of organizations are either in the planning or implementation stages of their Zero Trust journey, highlighting the widespread recognition of this approach as a security imperative [5]. This substantial adoption rate reflects the growing understanding that traditional perimeter-based security models no longer suffice in today's distributed IT environments.

This approach eliminates implicit trust based on network location, a critical shift given that 78% of organizations now view identity as their new perimeter. The report reveals that finance and banking organizations lead Zero Trust implementation, with 44% having reached advanced maturity levels that enforce strict identity verification for all resources [5]. Healthcare organizations follow closely behind at 38% advanced implementation, demonstrating the growing cross-industry recognition of Zero Trust principles. By applying micro-segmentation and least privilege access, these organizations create security architectures better aligned with the realities of modern work environments.

The implementation of Zero Trust frameworks varies significantly by region, with 35% of North American organizations having achieved advanced implementation compared to 24% in APAC and 18% in EMEA. This regional disparity in implementation maturity suggests different security priorities and resources across global markets [5]. Despite these variations, the report indicates a consistent year-over-year increase in Zero Trust adoption across all regions, with a 16% growth in advanced implementations since 2021, demonstrating the accelerating momentum toward this security approach.

3.2. Automate Identity Processes

Automation reduces human error and ensures consistent policy application across complex environments. CyberArk's analysis of identity security indicates that 51% of security professionals cite automation as critical for addressing the scale and complexity of modern identity management [6]. This recognition underscores how manual approaches can no longer keep pace with the expanding identity landscape, particularly as machine identities continue to proliferate across organizational environments.

Automated provisioning and deprovisioning based on HR events significantly reduce security risks associated with workforce changes. According to CyberArk's research, organizations leverage automation to address the 68% of security professionals who express concerns about keeping pace with the growing number of digital identities requiring management [6]. This statistic highlights the critical importance of implementing automated lifecycle processes that can scale effectively to meet organizational requirements while maintaining appropriate security controls.

CyberArk's research further reveals that 91% of security professionals express concern about the security risks associated with human identity management, while 89% report similar concerns regarding machine identities [6]. These parallel concerns highlight the importance of comprehensive automation approaches that address both human and non-human identities through structured workflows and consistent policy enforcement. Organizations implementing automated privileged access management workflows report significant improvements in their security posture, with automated approval processes ensuring appropriate oversight while reducing manual effort.

3.3. Establish Comprehensive Governance

Governance frameworks provide essential oversight for IAM operations, ensuring alignment with security objectives and compliance requirements. Okta's report indicates that 80% of organizations identify governance as a critical component of their Zero Trust strategy, with clear policies defining access requirements serving as the foundation for effective security controls [5]. This high prioritization demonstrates how governance has evolved from a compliance exercise to a fundamental security requirement.

Regular compliance audits and reporting mechanisms provide crucial validation of governance effectiveness. According to Okta's research, 33% of organizations now conduct quarterly assessments of their identity security posture, representing a 10% increase from the previous year [5]. This trend toward more frequent assessment reflects the growing recognition that governance cannot be an annual exercise in rapidly changing environments. Healthcare and financial services lead in governance maturity, with 41% and 39%, respectively, conducting monthly assessments of their identity security controls.

Risk-based approaches to access decisions represent a critical evolution in IAM governance. Okta's analysis reveals that 42% of organizations with advanced Zero Trust implementation have adopted contextual, risk-based access policies that dynamically adjust security requirements based on user behavior, device health, and environmental factors [5]. This approach represents a significant advancement over static policy models, allowing organizations to implement appropriate security controls without unnecessarily impeding legitimate user activities.

3.4. Implement Continuous Monitoring

Real-time monitoring detects suspicious activity before it escalates into serious security incidents. CyberArk's research highlights that 88% of organizations report that security professionals spend significant time manually monitoring identity security, creating operational inefficiencies while still leaving security gaps [6]. This statistic underscores the critical need for automated monitoring approaches that can provide comprehensive coverage while reducing operational burdens.

Anomalous access pattern detection represents a crucial monitoring capability. According to CyberArk's analysis, 89% of security professionals express concern about machine identity security risks, with 54% specifically highlighting the difficulty of detecting unauthorized access through machine identities [6]. This challenge emphasizes the importance of implementing advanced monitoring solutions capable of identifying unusual access patterns across both human and non-human identities, particularly as organizations increasingly rely on automated processes and service accounts.

Behavioral analytics to identify potential threats has emerged as a critical security capability. CyberArk's research indicates that 48% of organizations experience at least one security incident annually that specifically involves machine identities, highlighting the expanding attack surface requiring monitoring [6]. Organizations implementing advanced

analytics capabilities can detect these incidents more effectively, identifying subtle behavioral anomalies that might indicate compromise before significant damage occurs.

Automated alerts for security teams significantly improve incident response capabilities. According to CyberArk, 57% of organizations express concern about their ability to secure non-human identities, which now outnumber human identities by a factor of 45 to 1 in typical enterprise environments [6]. This massive imbalance makes manual monitoring approaches impractical, necessitating automated alert systems that can intelligently prioritize potential security incidents based on risk factors and provide security teams with the contextual information needed for effective response.

4. Regulatory Compliance and IAM

In today's complex regulatory landscape, robust Identity and Access Management (IAM) has become an essential component for maintaining compliance across various legal frameworks. Organizations face increasing scrutiny regarding how they manage access to sensitive information, with substantial penalties for non-compliance.

4.1. Meeting Key Regulatory Requirements

Effective IAM provides the foundation for addressing requirements across multiple regulatory frameworks. According to Simeio's IAM Maturity Benchmark research, only 10% of organizations have reached a mature capability in IAM implementation, while 90% remain at basic or developing stages, creating significant compliance and security challenges [7]. This maturity gap exposes organizations to substantial regulatory risks, particularly as identity-related threats continue to evolve in sophistication.

The General Data Protection Regulation (GDPR) requires strong controls over personal data access, with potential penalties of up to €20 million or 4% of global annual revenue for serious violations. Simeio's analysis reveals that organizations at Level 3 or above in IAM maturity are 2.7 times more likely to maintain continuous GDPR compliance compared to those at lower maturity levels [7]. The research further indicates that 67% of organizations still struggle with fundamental access governance processes, such as access certification and segregation of duties, creating significant GDPR compliance gaps. This direct connection between IAM maturity and regulatory compliance underscores the critical importance of implementing strong identity governance practices.

The Health Insurance Portability and Accountability Act (HIPAA) mandates the protection of patient health information, requiring healthcare organizations to implement strict access controls and maintain detailed audit trails. According to Syteca's Data Breach Investigation Best Practices, 72% of healthcare organizations experienced at least one data breach in the past year, with 43% of these incidents involving inappropriate access to protected health information [8]. Organizations with comprehensive identity security programs report 55% faster detection of unauthorized access attempts, significantly reducing the potential scope and impact of HIPAA violations. The research further notes that healthcare organizations implementing privileged access management solutions experience 39% fewer breaches involving administrative credentials compared to those without such controls.

The Payment Card Industry Data Security Standard (PCI-DSS) establishes detailed requirements for protecting payment card data, with specific controls focused on user identification, authentication, and access. Simeio's benchmark data indicates that 76% of organizations struggle with maintaining continuous PCI-DSS compliance due to challenges with access recertification and privilege management [7]. Financial services organizations with mature IAM implementations report 31% fewer audit findings related to requirements 7 and 8 of the PCI-DSS framework, which specifically addresses access control and user identification. This significant improvement demonstrates the direct impact of IAM maturity on PCI compliance readiness and sustainability.

The Sarbanes-Oxley Act (SOX) requires stringent controls over financial reporting systems to ensure data integrity and prevent fraud. Syteca's investigation data reveals that 64% of SOX deficiencies involve inadequate access controls, with particular challenges in managing segregation of duties and privileged access to financial systems [8]. Organizations implementing automated access governance solutions reduce the time required for SOX audit preparation by 27% while simultaneously improving the quality of evidence provided to auditors. This dual benefit of efficiency and effectiveness makes IAM a critical enabler for sustainable SOX compliance.

5. Industry Applications

5.1. Financial Services

Financial institutions face an evolving threat landscape while managing strict regulatory requirements across multiple jurisdictions. According to Simeio's industry-specific analysis, financial services organizations achieve the highest average IAM maturity score of 2.6 on a 5-point scale, reflecting the sector's recognition of identity as a critical security domain [7]. Despite this relatively strong performance, 59% of financial institutions still operate at or below the "Defined" maturity level, indicating significant room for improvement in their identity security programs.

Privileged access management for critical systems represents a particular focus area for financial institutions. Syteca's research indicates that 84% of data breaches in financial services involve privileged credential abuse or misuse, highlighting the critical importance of controlling administrative access [8]. Financial organizations implementing comprehensive PAM solutions report 42% fewer security incidents involving privileged accounts compared to those with basic password vault implementations. This substantial reduction in risk exposure demonstrates the value of advanced PAM capabilities, such as just-in-time access provisioning and session monitoring in financial environments.

Granular controls for trading platforms and customer information systems have become increasingly important for financial institutions. According to Simeio, only a few organizations in the financial sector currently have granular entitlement management capabilities (ABAM - Attribute-Based Access Management), with just 8% reaching Level 4 or 5 maturity in this critical capability [7]. Organizations implementing these advanced access controls report 23% fewer incidents of inappropriate data access compared to those using traditional role-based approaches. Financial institutions with mature entitlement management capabilities complete access reviews 35% faster while identifying 27% more inappropriate access rights, demonstrating the dual benefits of improved security and operational efficiency.

Fraud detection through behavioral monitoring has emerged as a critical IAM capability for financial services organizations. Syteca's analysis indicates that financial institutions implementing user and entity behavior analytics (UEBA) detect anomalous account activity 47% faster than those using traditional rule-based approaches [8]. Organizations leveraging machine learning for fraud detection experience a 31% reduction in false positives, significantly improving both security effectiveness and customer experience. Financial institutions with mature behavioral monitoring capabilities prevent an average of $3.4 million in potential fraud losses annually, demonstrating the substantial return on investment from these advanced IAM capabilities.

5.2. Healthcare

Healthcare organizations face the dual challenge of securing highly sensitive patient information while ensuring appropriate access to clinical care. According to Simeio's benchmark research, healthcare providers score an average IAM maturity of 2.3 on a 5-point scale, slightly below the cross-industry average of 2.4 [7]. This relatively low maturity is particularly concerning given that 60% of healthcare breaches involve privileged users, highlighting the critical need for improved identity security in this highly regulated sector.

Context-aware access for clinical staff has become increasingly important for healthcare organizations. Syteca's research indicates that 66% of healthcare providers still rely primarily on role-based access control models that lack the granularity and flexibility needed for dynamic clinical environments [8]. Organizations implementing context-aware authentication report 29% fewer instances of inappropriate access to electronic health records while maintaining clinical workflow efficiency. This improvement demonstrates how advanced access models can balance security requirements with the operational demands of patient care environments.

Emergency access protocols for critical care situations represent a unique healthcare requirement. According to Simeio, only 24% of healthcare organizations have implemented fully automated emergency access workflows with appropriate monitoring and governance capabilities [7]. Organizations with mature emergency access protocols reduce care delays related to access issues by 43% while maintaining comprehensive audit trails for compliance purposes. This balance between immediate access and governance enables healthcare providers to address urgent clinical needs without compromising their overall security posture.

Patient portal security for personal health information has become increasingly important as healthcare organizations expand their digital engagement channels. Syteca's data indicates that 77% of healthcare providers experienced at least one patient portal security incident in the past year, with credential theft representing the most common attack vector [8]. Organizations implementing multi-factor authentication for patient portals reduce unauthorized access attempts

by 67% compared to those relying solely on username and password authentication. Healthcare providers with advanced identity verification capabilities for patient access report a 41% increase in patient satisfaction with digital services, demonstrating the dual benefits of improved security and enhanced patient experience.

5.3. Government

Government agencies manage highly sensitive information while operating in complex multi-agency environments with stringent compliance requirements. According to Simeio's benchmark, government organizations score an average IAM maturity of 2.2 on a 5-point scale, falling below the cross-industry average of 2.4 [7]. This maturity gap is particularly concerning given that government agencies face unique security challenges, including sophisticated nation-state threats and complex compliance requirements spanning multiple regulatory frameworks.

Clearance-based access controls form the foundation of government information security. Simeio's research indicates that only 31% of government agencies have implemented automated clearance verification as part of their access governance processes, with the majority still relying on manual verification methods [7]. Agencies with mature clearance management capabilities report 35% fewer instances of inappropriate access to classified information, demonstrating the security benefits of automated approaches. The research further notes that government organizations with advanced authorization models reduce the time required for access changes by 43%, significantly improving operational efficiency in these complex environments.

Physical and logical access integration has become increasingly important for government security. According to Syteca, 81% of government security incidents involving former employees could have been prevented through proper integration of physical and logical access controls [8]. Agencies implementing unified identity governance frameworks that span both physical and digital access points reduce security gaps related to personnel changes by 54%. Government organizations with mature physical-logical access integration identify potential insider threats an average of 6.2 days faster than those maintaining separate systems, significantly reducing the window of vulnerability following personnel status changes.

Cross-agency federation for collaborative operations enables secure information sharing while maintaining appropriate access controls. Simeio's analysis indicates that only 26% of government organizations have reached advanced maturity in identity federation capabilities, creating significant challenges for secure inter-agency collaboration [7]. Agencies implementing comprehensive federation frameworks reduce the time required for cross-agency project initiation by 37% while maintaining appropriate security controls. According to Syteca, government organizations with mature federation capabilities experience 45% fewer security incidents related to external partner access, demonstrating how advanced IAM approaches can simultaneously improve both security and operational efficiency in complex multi-agency environments [8].

5.4. Emerging Trends in IAM

The Identity and Access Management landscape continues to evolve rapidly in response to changing business requirements, technological advancements, and emerging security challenges. Organizations are increasingly adopting innovative approaches to identity management that offer greater flexibility, security, and user experience improvements while addressing the limitations of traditional IAM frameworks.

5.5. Identity-as-a-Service (IDaaS)

Cloud-based IAM solutions have gained significant traction as organizations accelerate their digital transformation initiatives and migrate workloads to cloud environments. According to Gartner's Market Guide for Identity-First Security, by 2026, 90% of organizations will be using some form of cloud-delivered IAM capabilities to meet security challenges in a hybrid world, a significant increase from approximately 60% in 2022 [9]. This substantial growth reflects the compelling business case for cloud-delivered identity services, as organizations recognize the limitations of traditional on-premises IAM solutions in addressing the security requirements of increasingly distributed IT environments.

Simplified deployment across distributed environments represents a key driver for IDaaS adoption. Gartner's research indicates that identity-first security has emerged as a strategic imperative, with identity becoming the new security perimeter in today's hybrid and multi-cloud environments [9]. This shift is particularly evident in the rapid adoption of cloud access security broker (CASB) technologies, with 92% of organizations either using or planning to implement CASB solutions to protect their expanding cloud footprints. The research further highlights how cloud-delivered identity

services enable organizations to implement consistent security controls across distributed IT environments without the complexity and management overhead associated with traditional deployment models.

Subscription models aligning costs with actual usage have transformed IAM economics, shifting expenditures from capital to operational budgets. According to Zluri's analysis of identity and access management trends, 87% of business and security leaders cite operational cost reduction as a primary driver for adopting cloud-based IAM solutions [10]. These subscription-based models enable organizations to scale their identity security capabilities according to business needs while avoiding the substantial upfront investments associated with traditional on-premises deployments. The research further indicates that 73% of organizations report improved budgeting predictability after transitioning to consumption-based IAM pricing models, facilitating more effective financial planning and resource allocation.

Integrated security features with regular updates provide organizations with enhanced protection against evolving threats. Gartner's analysis reveals that modern identity architectures must be continuously updated to address emerging attack vectors, with cloud-delivered solutions offering significant advantages in this regard [9]. The research specifically highlights how IDaaS providers can rapidly deploy security enhancements in response to evolving threats such as adversary-in-the-middle (AiTM) phishing campaigns, which increasingly bypass traditional MFA implementations. According to Gartner, 60% of organizations will strengthen their authentication methods with advanced approaches such as device binding, location analysis, behavioral analytics, and continuous risk assessment by 2025 to counter these sophisticated attacks – capabilities that are more readily available and implemented through cloud-delivered identity platforms.

5.6. Adaptive Authentication

Risk-based approaches to authentication have emerged as a critical capability for balancing security with user experience. Zluri's comprehensive analysis indicates that 82% of organizations now consider adaptive authentication essential for protecting their digital assets while maintaining user productivity [10]. This growing recognition of the limitations of static authentication models reflects the reality that traditional password-based approaches no longer provide adequate protection against increasingly sophisticated credential-based attacks. The research further reveals that organizations implementing adaptive authentication experience an average 70% reduction in account compromise incidents while simultaneously reporting a 60% decrease in authentication-related help desk calls.

Contextual factors such as location, device, and time increasingly inform authentication decisions, enabling more nuanced security responses. According to Gartner, by 2025, 60% of organizations will use authentication methods that integrate contextual and behavioral signals to enable adaptive access decisions based on calculated risk [9]. This trend represents a significant evolution from traditional binary authentication models toward continuous, risk-based approaches that can dynamically adjust security requirements based on the specific context of each access request. The research specifically highlights how these advanced authentication mechanisms enable organizations to implement proportional security controls that align protection measures with the risk level of specific transactions or resource access requests.

Behavioral biometrics detect anomalies in user patterns, providing continuous validation of user identity without explicit authentication challenges. Zluri's analysis indicates that 65% of organizations plan to implement some form of behavioral analytics within their authentication frameworks by 2024, with financial services and healthcare leading this adoption at 78% and 71%, respectively [10]. These implementations leverage advanced machine learning algorithms to establish baseline user behavior patterns and identify potential compromise through the detection of anomalous activities. The research further indicates that organizations implementing behavioral biometrics report a 55% improvement in their ability to detect account takeover attempts while reducing false positives by approximately 40% compared to rule-based detection approaches.

Continuous authentication throughout sessions represents a significant advancement over traditional point-in-time validation. According to Gartner, 40% of large enterprises will adopt continuous and adaptive authentication by 2025 to address the limitations of static credential verification [9]. This approach represents a fundamental shift from treating authentication as a discrete event to viewing it as an ongoing process that continuously validates user identity throughout active sessions. The research specifically highlights how this evolution enables organizations to maintain appropriate security controls without unnecessarily disrupting legitimate user activities, creating a balanced approach that enhances both security posture and user experience. Zluri's analysis reinforces this trend, noting that organizations implementing continuous authentication report an average 45% reduction in session hijacking incidents while simultaneously reducing user friction by approximately 30% [10].

5.7. Decentralized Identity

Blockchain and self-sovereign identity technologies are reshaping identity management approaches, offering new models for portable, user-controlled digital identity. Zluri's emerging technology analysis indicates that 51% of organizations are investigating decentralized identity solutions, with 23% already engaged in active pilot programs [10]. This growing interest reflects a recognition of the limitations of centralized identity models in addressing the requirements of increasingly complex digital ecosystems. The research further indicates that organizations implementing decentralized approaches report a 47% reduction in identity verification costs across their partner networks and a significant improvement in user satisfaction with identity-related processes.

User control over personal identity information represents a fundamental shift from traditional organization-controlled identity models. According to Zluri, 76% of consumers express concern about how their personal data is managed by organizations, with 82% indicating a preference for greater control over their digital identities [10]. This growing consumer awareness of data privacy issues is driving significant changes in how organizations approach identity management, with 68% of businesses reporting that privacy considerations now substantially influence their identity strategy and technology decisions. The research further reveals that organizations implementing user-centric identity approaches report a 43% improvement in customer trust metrics and a 38% increase in willingness to share personal information for value-added services.

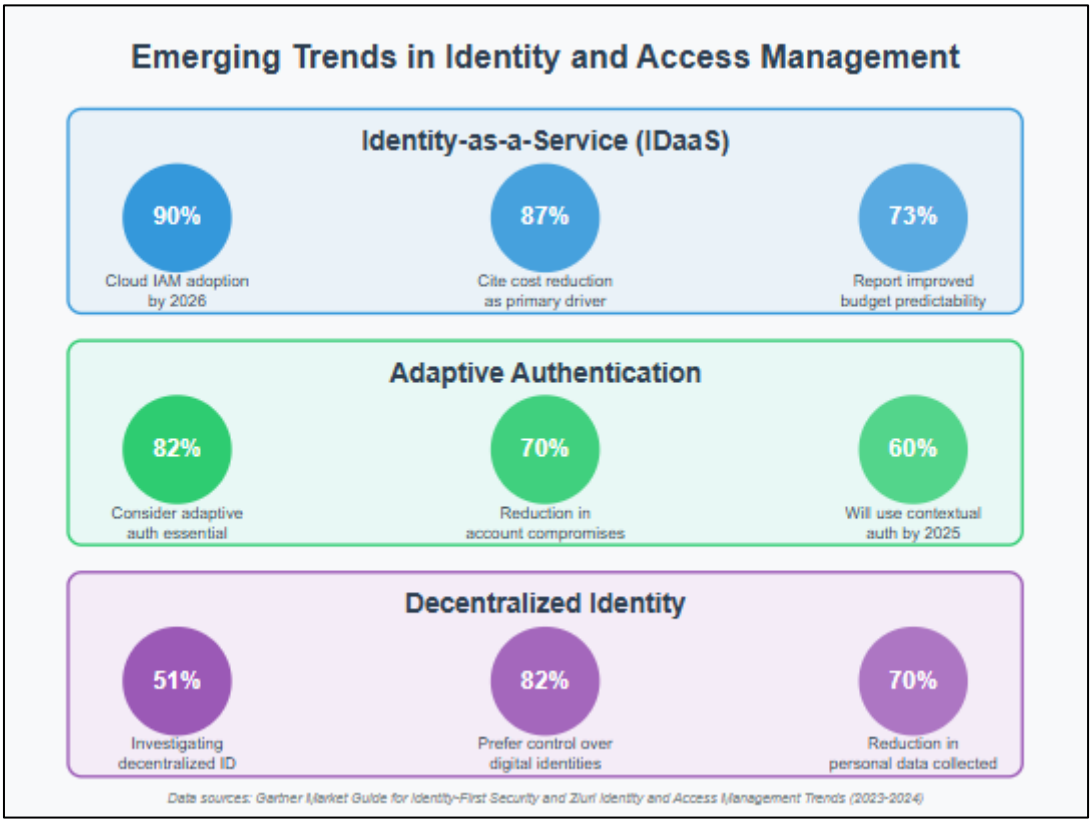

Figure 2 Emerging Trends in Identity and Access Management

Reduced reliance on centralized identity providers minimizes catastrophic breach risks and enables more flexible identity ecosystems. Gartner's research indicates that by 2025, 30% of large enterprises will implement self-sovereign identity solutions for specific use cases, such as customer onboarding or partner access [9]. This trend represents a significant departure from traditional federated identity models that rely on centralized identity providers, moving toward more distributed approaches that eliminate single points of failure and enable greater ecosystem flexibility. The research specifically highlights how these decentralized models improve resilience against provider outages or compromises while facilitating more seamless identity verification across organizational boundaries.

Improved privacy through selective disclosure enables users to share only the minimum necessary information for specific transactions. According to Zluri, 64% of organizations cite enhanced privacy capabilities as a primary driver for exploring decentralized identity technologies [10]. These solutions leverage cryptographic techniques such as zero-

knowledge proofs to enable verification of claims without exposing underlying data, significantly reducing privacy risks. The research further indicates that implementations supporting selective disclosure reduce the amount of personal data collected during typical transactions by approximately 70%, addressing growing privacy concerns while maintaining the ability to perform necessary identity verification. This capability is particularly valuable in highly regulated industries such as healthcare and financial services, where organizations must balance privacy requirements with strict compliance obligations.

6. Conclusion

Identity and Access Management has transcended its origins as a basic security function to become a strategic enabler of digital transformation. Organizations implementing comprehensive IAM frameworks gain enhanced security posture alongside improved operational efficiency, streamlined compliance processes, and secure collaboration capabilities. As threat landscapes continue to evolve, the core principles of strong identity verification, least privilege access, and continuous monitoring remain essential protections for organizational assets. By embracing IAM best practices and adopting emerging technologies like cloud-delivered identity services, adaptive authentication, and self-sovereign identity solutions, organizations can build resilient security architectures capable of addressing both current and future challenges in our increasingly interconnected digital ecosystem.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abi Tyas Tunggal, "What is the Cost of a Data Breach in 2023?" UpGuard, 2025. [Online]. Available: https://www.upguard.com/blog/cost-of-data-breach

[2] David Collinson et al., "Market Guide for Identity Governance and Administration," Gartner Research, Inc., 2020. [Online]. Available: https://www.gartner.com/en/documents/3994045

[3] F5 Labs, "2023 Identity Threat Report: The Unpatchables," F5, Inc., 2023. [Online]. Available: https://www.f5.com/labs/articles/threat-intelligence/2023-identity-threat-report-the-unpatchables

[4] Microsoft Security, "Microsoft Digital Defense Report Executive Summary Building and improving cyber resilience," Microsoft, 2023. [Online]. Available: https://www.itsoluzioni.it/wp-content/uploads/2023/12/MDDR_executivesummary_Oct2023.pdf

[5] Okta, "The State of Zero Trust Security in Global Organizations," Okta, Inc. [Online]. Available: https://www.okta.com/resources/reports/state-of-zero-trust-security-in-global-organizations/

[6] Scott Carter "The Urgent Reality of Machine Identity Security in 2025," CyberArk, 2025. [Online]. Available: https://www.cyberark.com/resources/blog/the-urgent-reality-of-machine-identity-security-in-2025

[7] Simeio, "IAM Maturity Benchmark: Is Your Business' Identity Security Too Immature?" Simeio Solutions, LLC. [Online]. Available: https://simeio.com/iam/iam-maturity-benchmark-is-your-business-identity-security-too-immature/

[8] Liudmyla Pryimenko, "Data Breach Response and Investigation: 8 Steps for Efficient Remediation," Syteca, 2024. [Online]. Available: https://www.syteca.com/en/blog/data-breach-investigation-best-practices

[9] Erik Wahlstrom et al., "2025 Planning Guide for Identity and Access Management," Gartner, Inc., 2024. [Online]. Available: https://www.gartner.com/en/documents/5823247

[10] Zluri, "7 Identity and Access Management Trends," Zluri, 2024. [Online]. Available: https://www.zluri.com/blog/identity-and-access-management-trends