Sarcouncil Journal of Engineering and Computer Sciences

**ISSN(Online): 2945-3585**

Volume- 04| Issue- 07| 2025

**Research Article** **Received:** 19-06-2025| **Accepted:** 10-07-2025 | **Published:** 29-07-2025

# The Critical Role of Identity and Access Management in Modern Enterprise Security Frameworks

***Deepak Pandey***
*Simeio Solutions LLC, USA*

**Abstract:** This article examines the pivotal role of Identity and Access Management (IAM) in contemporary enterprise security architectures amid escalating cybersecurity challenges. As organizations embrace cloud migration, remote work models, and expanding digital supply chains, traditional security perimeters have dissolved, positioning identity as the new security boundary. The article explores how IAM systems—comprising identity management, authentication mechanisms, authorization protocols, and auditing capabilities—serve as foundational elements for implementing Zero Trust security models through continuous authentication, contextual authorization, fine-grained access control, and privileged access management. It further investigates the complex regulatory landscape governing identity management across sectors and jurisdictions, highlighting how organizations must navigate compliance requirements while maintaining operational efficiency. Despite IAM's critical importance, implementation challenges persist across technical, operational, and cultural dimensions, including legacy system integration, user experience considerations, organizational structures, skill gaps, scalability requirements, cost management, and change management. The article concludes that effective IAM implementation requires organizations to view identity governance not merely as a technical solution but as a strategic security enabler that aligns with business objectives and comprehensive risk management frameworks.

**Keywords:** Identity Governance, Zero Trust Architecture, Regulatory Compliance, Enterprise Security, Authentication Frameworks

## INTRODUCTION

In today's increasingly interconnected digital ecosystem, organizations face unprecedented security challenges that threaten the confidentiality, integrity, and availability of critical assets. The modern enterprise environment, characterized by cloud migration, remote workforce models, and expanding digital supply chains, has dramatically expanded the attack surface available to malicious actors. According to Verizon's Data Breach Investigations Report, credential-based attacks continue to dominate the threat landscape, with phishing and social engineering tactics being primary vectors for identity compromise (Verizon, 2025). The report highlights that privileged credentials remain highly valuable targets, providing attackers with expanded access to sensitive systems and data.

Identity and Access Management (IAM) has emerged as a foundational component of enterprise security architectures within this complex risk landscape. Organizations implementing robust IAM programs demonstrate greater resilience against these prevalent attack patterns, as documented in recent industry analyses that correlate mature identity controls with improved security outcomes (Verizon, 2025). The Verizon report emphasizes that multi-factor authentication and privilege management remain among the most effective controls for mitigating identity-based attacks.

IAM encompasses the policies, processes, and technologies that enable organizations to manage digital identities and control access to resources based on established security policies. As highlighted in market research by IT Asset Management, enterprise IAM implementations must now accommodate complex hybrid environments spanning on-premises legacy systems and multiple cloud platforms (IT Asset Management). The significance of IAM has grown exponentially as traditional network perimeters dissolve, making identity the new security perimeter. This transformation has accelerated with the widespread adoption of remote work arrangements, creating scenarios where users access corporate resources from diverse locations and devices.

This paper examines the critical role of IAM within enterprise security frameworks, exploring its technical implementation patterns, integration with modern security paradigms, regulatory considerations, and organizational challenges. The market analysis from IT Asset Management indicates that IAM has become a strategic investment priority for security leaders, with spending trends reflecting the growing recognition of identity as a critical security domain (IT Asset Management). This growth encompasses solutions for identity governance, privileged access management, and customer identity management, demonstrating the expanding scope of IAM programs.





*Corresponding Author: Deepak Pandey

DOI- https://doi.org/10.5281/zenodo.16570105

As organizations continue their digital transformation journeys, understanding the strategic importance of robust identity governance becomes essential for effective risk management and operational resilience. The Verizon report underscores that organizations with mature IAM capabilities demonstrate more effective incident response capabilities and reduced dwell time for attackers, highlighting the correlation between identity governance maturity and overall security posture (Verizon, 2025). Meanwhile, industry analysis shows that leading organizations are increasingly integrating IAM with broader security frameworks such as Zero Trust architectures to create comprehensive defense models that better address contemporary threats (IT Asset Management).

## FUNDAMENTALS OF IAM ARCHITECTURE AND COMPONENTS

Identity and Access Management systems consist of several interconnected components that collectively facilitate the secure management of digital identities throughout their lifecycle. At its core, an IAM framework includes identity management, authentication mechanisms, authorization protocols, and comprehensive auditing capabilities. The Forrester Total Economic Impact study on IAM solutions highlights that organizations implementing comprehensive identity governance frameworks experience significant operational benefits alongside enhanced security outcomes, with measurable reductions in administrative overhead and security incidents (Forrester Research, 2020).

The identity management component establishes and maintains digital identities, encompassing processes for identity creation, modification, and deactivation. This component typically interfaces with authoritative sources such as Human Resource Management Systems (HRMS) to ensure identity data accuracy and consistency. Imprivata's implementations, as analyzed in the Forrester study, demonstrate that automated provisioning and deprovisioning workflows substantially reduce the time required for identity lifecycle management while minimizing security risks associated with orphaned accounts (Forrester Research, 2020). Authentication mechanisms verify claimed identities through various factors, ranging from knowledge-based approaches (passwords, security questions) to possession-based methods (security tokens, mobile devices) and inherence factors (biometrics). Modern authentication frameworks, such as the Fast Identity Online (FIDO) alliance standards, are increasingly prioritizing passwordless approaches to strengthen security while improving user experience. The Microsoft Digital Defense Report emphasizes that strong authentication represents one of the most effective controls against identity-based attacks, with multi-factor authentication significantly reducing the success rate of compromise attempts across Microsoft's monitored environments (Microsoft Security, 2024).

Authorization protocols determine access privileges associated with authenticated identities, implementing attribute-based or role-based access control models. These models enable fine-grained access decisions based on contextual factors, including user attributes, resource sensitivity, access location, and device characteristics. Microsoft's defense telemetry indicates that privilege escalation remains a primary objective for threat actors following initial compromise, highlighting the critical importance of implementing least-privilege access models and just-in-time privilege elevation (Microsoft Security, 2024). Finally, comprehensive auditing capabilities record identity-related events, providing visibility into authentication attempts, access decisions, privilege modifications, and administrative actions. The Microsoft Digital Defense Report emphasizes that identity-related signals have become foundational elements of modern security operations, with identity telemetry providing critical indicators of compromise that often precede more obvious attack manifestations (Microsoft Security, 2024).

These components interact through standardized protocols such as SAML, OAuth, OpenID Connect, and SCIM, facilitating interoperability across heterogeneous enterprise environments. Organizations implementing standardized identity federation frameworks, as documented in the Imprivata case studies, report substantial reductions in integration complexity and administrative overhead (Forrester Research, 2020). The architecture may be implemented through centralized, federated, or distributed models, each offering distinct advantages in terms of management complexity, scalability, and resilience. Microsoft's security guidance emphasizes that hybrid identity architectures have become the predominant deployment model, enabling organizations to balance legacy system requirements with cloud transformation initiatives



Publisher: SARC Publisher

while maintaining consistent identity governance across environments (Microsoft Security, 2024).

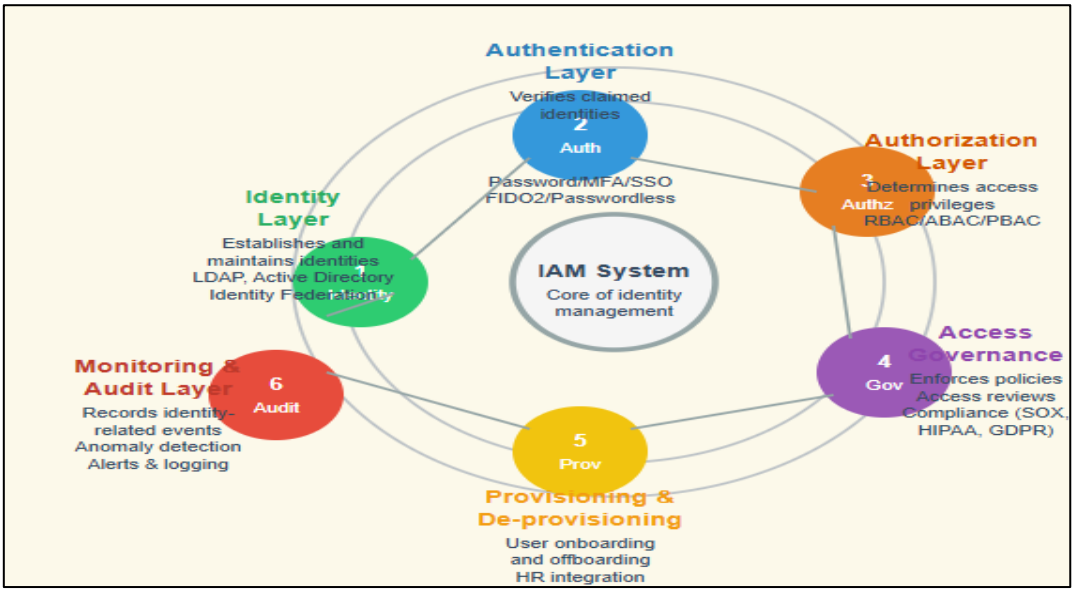


**Fig 1**: IAM Architecture and Components (Forrester Research, 2020; Microsoft Security, 2024)

## IAM AS THE FOUNDATION OF ZERO TRUST SECURITY MODELS

The traditional security paradigm of establishing a hardened perimeter around organizational assets has proven inadequate in addressing contemporary threats. Zero Trust architecture has emerged as a response to this challenge, advocating for a security model that eliminates implicit trust and continuously validates every access request regardless of source. NIST Special Publication 800-207 defines Zero Trust as "a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated," establishing that no actor, system, or service operating within or outside the security perimeter should be trusted by default (Rose, S. *et al.*, 2020). IAM serves as the cornerstone of effective Zero Trust implementation, providing the identity verification and access control mechanisms necessary for its execution. Gartner's analysis of Zero Trust Network Access emphasizes that robust identity verification represents the most critical capability for implementing Zero Trust architectures, with identity-based controls serving as the primary security boundary in modern Zero Trust environments (McQuaid, A. *et al.*, 2023).

Zero Trust principles—including "never trust, always verify," "assume breach," and "least privilege access"—rely heavily on robust identity governance. NIST's framework specifically positions subject (user and system) authentication and authorization as the foundational tenets of Zero Trust, establishing identity verification as the primary control through which all other security decisions flow (Rose, S. *et al.*, 2020). IAM enables the implementation of these principles through several critical mechanisms:

Continuous authentication represents a significant evolution beyond traditional session-based identity verification. Rather than one-time verification at the session initiation, IAM systems support ongoing authentication by continuously monitoring identity risk signals and prompting for additional verification when anomalies are detected. NIST's architectural guidance specifically emphasizes that authentication in Zero Trust models must be continuous rather than static, with ongoing validation of identity claims throughout the access lifecycle (Rose, S. *et al.*, 2020). This capability directly supports the Zero Trust principle of continuous verification, ensuring that access rights are consistently reassessed throughout the user's interaction with enterprise resources.

Contextual authorization further enhances the Zero Trust model by providing dynamic access decisions. IAM frameworks evaluate numerous contextual attributes when making access decisions, including device health, network characteristics, geolocation, time patterns, and behavior analytics. The Gartner analysis highlights that ZTNA (Zero Trust Network Access) solutions increasingly incorporate risk-based contextual factors into access decisions, enabling more granular control over resource access based on





**Publisher: SARC Publisher**

real-time assessment of security posture (McQuaid, A. *et al.*, 2023). This approach aligns with NIST's recommendation that authentication and authorization decisions incorporate context from multiple sources, including device status, network location, and behavioral patterns (Rose, S. *et al.*, 2020).

Fine-grained access control implements the principle of least privilege, restricting access rights to the minimum necessary for users to perform their job functions and thereby reducing the potential attack surface. NIST specifically identifies the principle of least privilege as a core tenet of Zero Trust Architecture, emphasizing that access to resources should be limited to only what is required for legitimate use (Rose, S. *et al.*, 2020). Gartner's analysis notes that leading Zero Trust implementations incorporate increasingly granular authorization models that restrict access at the application and data levels rather than providing broad network-level access (McQuaid, A. *et al.*, 2023). This microsegmentation approach directly supports the Zero Trust objective of minimizing implicit trust zones within the environment.

Privileged access management constitutes a specialized but critical component of Zero Trust IAM implementations. IAM includes specialized controls for managing privileged accounts that have elevated access to critical systems, implementing just-in-time access, session monitoring, and credential vaulting. NIST guidance recognizes that privileged access represents a particular challenge in Zero Trust environments, requiring enhanced controls beyond standard user authentication (Rose, S. *et al.*, 2020). The Gartner analysis specifically highlights privileged session management as a differentiating capability among mature ZTNA solutions, providing enhanced visibility and control over administrative actions (McQuaid, A. *et al.*, 2023). Organizations implementing comprehensive privileged access management as part of their Zero Trust strategy can significantly reduce the risk surface associated with administrative credentials.

The convergence of IAM and Zero Trust represents a paradigm shift from perimeter-based security to identity-centric approaches. This integration enables organizations to establish continuous trust verification while maintaining operational efficiency, positioning identity as the new control plane for security operations. Gartner identifies identity-centric security as a defining characteristic of advanced Zero Trust implementations, noting that leading organizations integrate identity governance with network, endpoint, and application controls to create comprehensive security frameworks (McQuaid, A. *et al.*, 2023). This perspective aligns with NIST's architectural tenets, which position identity verification as the logical foundation upon which other Zero Trust capabilities depend (Rose, S. *et al.*, 2020).

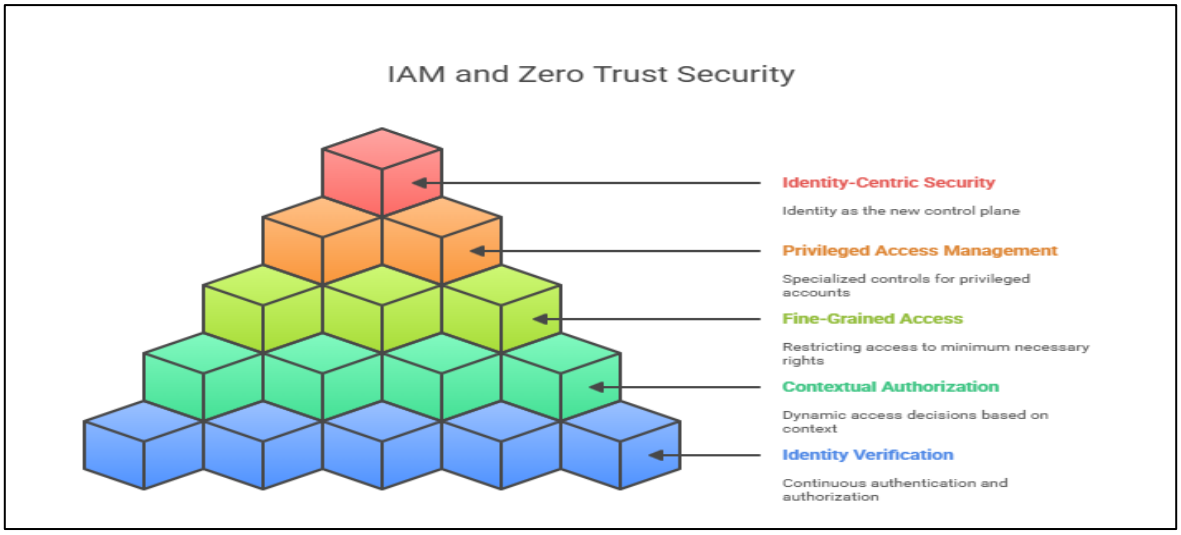


**Fig 2:** IAM and Zero Trust Security (Rose, S. *et al.*, 2020; McQuaid, A. *et al.*, 2023)

## REGULATORY COMPLIANCE AND IAM IMPLEMENTATION FRAMEWORKS

The regulatory landscape governing digital identity management has grown increasingly complex, with numerous frameworks establishing requirements for identity verification,



Publisher: SARC Publisher

authentication strength, privacy protection, and access governance. IAM implementations must align with these regulatory mandates while addressing industry-specific compliance requirements. According to Zluri's comprehensive IAM framework analysis, organizations implementing structured identity governance programs demonstrate significantly higher compliance success rates while reducing audit preparation efforts by streamlining evidence collection and control documentation (Panda, C. 2024).

The National Institute of Standards and Technology (NIST) has published several influential guidelines that shape IAM implementations, including Special Publication 800-63 (Digital Identity Guidelines), which defines identity assurance levels and authentication assurance levels. Zluri's framework analysis highlights how NIST guidelines have become the de facto standard for IAM implementations across sectors, with their identity assurance level (IAL) and authenticator assurance level (AAL) classifications providing a structured approach to matching authentication strength with data sensitivity (Panda, C. 2024). Similarly, the European Union's General Data Protection Regulation (GDPR) establishes stringent requirements for identity data protection, including principles of data minimization, purpose limitation, and the right to be forgotten. Microsoft's identity governance documentation emphasizes that GDPR compliance necessitates comprehensive identity data management capabilities, including the ability to discover, classify, and manage access to personal information across diverse systems (Billmath, *et al.,* 2025).

Industry-specific regulations such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare, the Payment Card Industry Data Security Standard (PCI DSS) for financial services, and the Federal Risk and Authorization Management Program (FedRAMP) for government agencies further define IAM requirements within their respective domains. The Zluri IAM framework outlines how these specialized regulatory regimes necessitate tailored IAM implementations, with healthcare organizations requiring specialized patient identity management capabilities and financial institutions implementing enhanced transaction monitoring for identity-related fraud detection (Panda, C. 2024). These regulatory frameworks, while diverse in scope, collectively emphasize several core principles:

Strong authentication requirements have become ubiquitous across regulatory frameworks, with multi-factor authentication increasingly mandated for sensitive operations or privileged access. Microsoft's identity governance guidance specifically addresses how modern compliance frameworks require adaptive authentication policies that balance security requirements with usability considerations, enabling organizations to implement risk-based authentication that escalates verification requirements based on access context (Billmath, *et al.,* 2025).

The principle of least privilege appears consistently throughout regulatory guidance, mandating organizations to restrict access rights to the minimum necessary for legitimate business functions. Zluri's framework analysis notes that implementing least privilege access models requires systematic role engineering and entitlement mapping, enabling organizations to align access privileges with functional responsibilities and compliance requirements (Panda, C. 2024). This approach directly supports regulatory mandates for access minimization while improving operational security posture.

Access review processes represent a critical compliance requirement across regulatory frameworks, with regular certification of access rights being mandatory to prevent privilege accumulation. Microsoft's identity governance platform emphasizes that effective access review programs must balance thoroughness with reviewer efficiency, using analytics and machine learning to prioritize high-risk access combinations for intensive manual review while streamlining routine certifications (Billmath *et al.,* 2025). This risk-based approach enables organizations to focus compliance efforts on areas of greatest regulatory concern.

Identity lifecycle management controls focus on timely provisioning and deprovisioning of access, addressing regulatory concerns regarding orphaned accounts and lingering privileges. The Zluri IAM framework identifies automated lifecycle management as a foundational compliance capability, enabling organizations to demonstrate to regulators that access rights are consistently aligned with employment status and role changes (Panda, C. 2024). Microsoft's governance approach further emphasizes the importance of



**Publisher: SARC Publisher**

integrating identity lifecycle management with human resources systems to ensure synchronization between employment events and access privileges (Billmath, *et al.*, 2025).

Audit trails provide the evidentiary foundation for compliance verification, with comprehensive logging and monitoring of identity and access events enabling both detective controls and forensic investigation capabilities. Microsoft's governance documentation highlights how modern compliance frameworks require not only comprehensive audit capture but also analytical capabilities that can identify patterns indicative of compliance violations or security incidents (Billmath, *et al.*, 2025). These capabilities enable organizations to demonstrate proactive compliance monitoring rather than reactive response.

Organizations must navigate this complex regulatory ecosystem while implementing IAM solutions that balance compliance requirements with operational efficiency. Framework alignment often necessitates the development of comprehensive identity governance policies, regular compliance assessments, and continuous control monitoring. Zluri's implementation guidance recommends that organizations adopt a risk-based approach to compliance, prioritizing IAM controls that address the most significant regulatory risks while aligning implementation priorities with business objectives (Panda, C. 2024). Microsoft's governance framework similarly emphasizes the importance of integrating compliance requirements into broader identity governance programs, enabling organizations to address regulatory mandates within a comprehensive security and risk management strategy (Billmath, *et al.*, 2025).

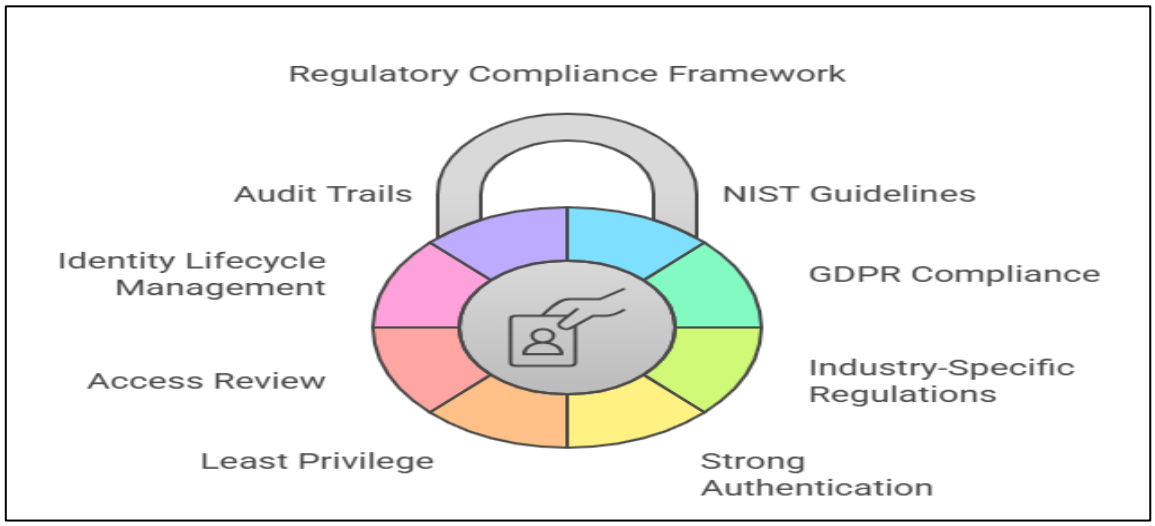


**Fig 3**: Regulatory Compliance Framework (Panda, C. 2024; Billmath *et al.*, 2025)

## ORGANIZATIONAL CHALLENGES AND IMPLEMENTATION CONSIDERATIONS

Despite the critical importance of IAM, organizations face significant challenges in implementing effective identity governance frameworks. These challenges span technical, operational, and cultural dimensions, requiring a multifaceted approach to address them effectively. According to Oracle's analysis of IAM implementation challenges, organizations increasingly struggle with the expanding complexity of identity ecosystems, particularly as digital transformation initiatives accelerate the adoption of cloud services and remote work models (Chen, M. 2024).

One primary challenge involves the integration of IAM systems with legacy applications that lack support for modern authentication protocols. Organizations often maintain complex environments with applications developed over decades, creating technical debt that complicates identity standardization efforts. Oracle identifies heterogeneous IT environments as a fundamental barrier to IAM success, noting that enterprises typically struggle to maintain consistent identity controls across on-premises legacy systems, SaaS applications, and multi-cloud infrastructure (Chen, M. 2024). This heterogeneity necessitates the implementation of identity proxies, application gateways, or custom connectors that bridge modern IAM platforms with legacy systems. KuppingerCole's Leadership Compass for Identity



**Publisher: SARC Publisher**

Governance and Administration emphasizes that successful IAM implementations must prioritize comprehensive connectivity capabilities, evaluating solutions based on their ability to integrate with diverse application ecosystems through both standard protocols and specialized connectors (Deshpande, N. 2024).

User experience considerations present another challenge, as stringent security controls can create friction that impacts productivity and encourages workarounds. Oracle's implementation research highlights how excessive authentication requirements and cumbersome access request processes frequently lead to user resistance, with employees developing shadow IT solutions to circumvent perceived barriers to productivity (Chen, M. 2024). Balancing security requirements with usability necessitates thoughtful implementation of adaptive authentication flows, single sign-on capabilities, and user-friendly self-service tools. The KuppingerCole analysis identifies user experience as an increasingly critical evaluation factor for IAM solutions, with leading platforms now emphasizing intuitive interfaces, streamlined request workflows, and consumer-grade mobile experiences (Deshpande, N. 2024).

Organizational structures can also impede effective IAM implementation, particularly when identity governance responsibilities are fragmented across multiple teams or departments. Oracle identifies organizational silos as a significant barrier to IAM success, with fragmented responsibility models creating policy inconsistencies and implementation gaps (Chen, M. 2024). Successful IAM programs typically require clear governance structures with defined roles and responsibilities spanning IT operations, security, compliance, and business units. The KuppingerCole Leadership Compass emphasizes that effective identity governance requires organizational alignment across technical teams and business stakeholders, with successful deployments demonstrating strong executive sponsorship and clear lines of accountability (Deshpande, N. 2024).

Additionally, organizations must address skill gaps within their workforce, as effective IAM implementation requires specialized expertise in identity protocols, directory services, authentication methods, and access governance processes. Oracle's assessment of implementation challenges highlights that the technical complexity of modern IAM solutions creates significant knowledge barriers for many organizations, with specialized skills required for integration, policy development, and ongoing administration (Chen, M. 2024). This expertise gap often necessitates investments in training programs, external consultancies, or managed service partnerships. KuppingerCole's market analysis indicates a growing trend toward managed service delivery models, with organizations increasingly leveraging specialized service providers to supplement internal capabilities, particularly for advanced functionality such as identity analytics and role management (Deshpande, N. 2024).

Implementation considerations should also account for scalability requirements, particularly in organizations experiencing rapid growth or frequent mergers and acquisitions. IAM architectures must accommodate identity integration from disparate sources while maintaining consistent security policies and access controls across the expanded environment. Oracle's implementation guidance emphasizes the importance of designing IAM architectures with future growth in mind, avoiding short-term decisions that create scalability constraints as organizational requirements evolve (Chen, M. 2024). The KuppingerCole evaluation framework specifically assesses IAM solutions for scalability characteristics, including performance with large user populations, multi-tenant capabilities, and the ability to maintain consistent policy enforcement across distributed environments (Deshpande, N. 2024).

Cost management represents another significant challenge in IAM implementations, with organizations frequently encountering unexpected expenses related to integration complexity, customization requirements, and ongoing administration. Oracle identifies total cost of ownership as a critical consideration in IAM planning, noting that initial licensing costs often represent only a fraction of the true implementation expense (Chen, M. 2024). KuppingerCole's analysis emphasizes the importance of comprehensive cost modeling that includes not only software licensing but also integration services, training, and ongoing operational expenses, with particular attention to the resource requirements for maintaining custom integrations and policies (Deshpande, N. 2024).

Finally, organizations must address change management considerations to ensure successful adoption of new identity processes and controls.



Publisher: SARC Publisher

Oracle's implementation framework highlights that even technically sound IAM deployments can fail without effective organizational change management, including stakeholder education, clear communication of benefits, and phased implementation approaches that allow for adjustment periods (Chen, M. 2024). The KuppingerCole Leadership Compass recommends that organizations evaluate not only technical capabilities but also vendor implementation methodologies, including change management frameworks, training programs, and deployment best practices that minimize organizational disruption (Deshpande, N. 2024).

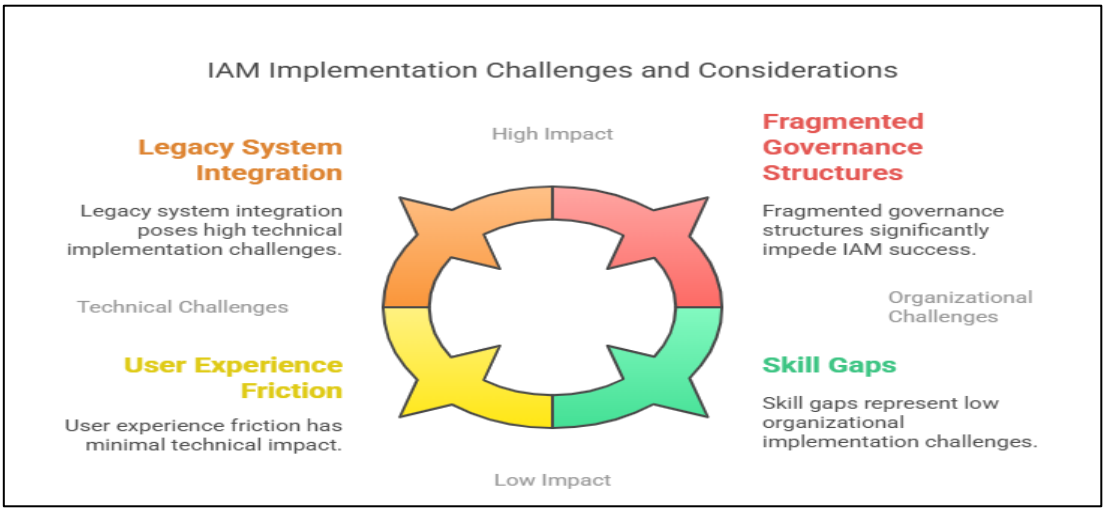


**Fig 4**: IAM Implementation Challenges and Considerations (Chen, M. 2024; Deshpande, N. 2024)

## CONCLUSION

Identity and Access Management has transcended its origins as a tactical IT function to emerge as a strategic security enabler that underpins modern enterprise security architectures. As organizations navigate increasingly complex digital transformations, cloud migrations, and evolving threat landscapes, the centrality of identity in security frameworks will only intensify, with IAM effectiveness directly influencing security posture, operational efficiency, and compliance standing. The trajectory of IAM points toward greater integration of artificial intelligence and machine learning capabilities, enabling adaptive security postures that respond dynamically to changing risk conditions, while identity analytics increasingly inform security decisions with behavioral patterns establishing baseline activity profiles against which anomalies can be detected. For security leaders and practitioners, success requires conceptualizing IAM not as a mere technical implementation but as a comprehensive governance framework aligned with business objectives and risk management strategies, enabling organizations to achieve greater resilience against evolving threats while facilitating business agility in dynamic market conditions. As the digital identity landscape continues to evolve through emerging standards such as decentralized identity frameworks, effective IAM will remain the critical differentiator between organizations that merely react to security challenges and those that proactively address them through strategic identity governance.

## REFERENCES

1. Verizon, "Data Breach Investigations Report." *Verizon Business* "(2025). https://www.verizon.com/business/resources/reports/dbir/
2. IT Asset Management, "Market Guide: Identity & Access Management (IAM)." *IT Asset Management Marketplace.* https://marketplace.itassetmanagement.net/marketplace/market-guides/market-guide-identity-access-management-iam/
3. Forrester Research, "The Total Economic Impact™ Of Imprivata Identity Access Management Solutions." *Imprivata*, (2020). Available: https://security.imprivata.com/rs/413-FZZ-310/images/IAM-AR-Forrester-Total-Economic-Impact-Report-0520.pdf
4. Microsoft Security, "Microsoft Digital Defense Report 2024." *Microsoft Corporation*.(2024) https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf





**Publisher: SARC Publisher**

5. Rose, S. *et al.,* "Zero trust architecture." *NIST special publication* 800.207 (2020): 800-207.
6. McQuaid, A. *et al.,* "Market Guide for Zero Trust Network Access." *Gartner,* (2023). https://www.gartner.com/en/documents/4632099
7. Panda, C. "Identity and Access Management Framework: An Overview," *Zluri,* (2024). https://www.zluri.com/blog/identity-and-access-management-framework
8. Billmath *et al.,* "What is Microsoft Entra ID Governance?" *Microsoft Learn,* (2025). https://learn.microsoft.com/en-us/entra/id-governance/identity-governance-overview
9. Chen, M. "Top 7 Identity and Access Management Challenges to Solve." *Oracle,* (2024). https://www.oracle.com/in/security/identity-management/iam-challenges/
10. Deshpande, N. "Identity Governance and Administration," *KuppingerCole,* (2024). https://www.kuppingercole.com/research/lc80832/identity-governance-and-administration

**Source of support:** Nil; **Conflict of interest:** Nil.

**Cite this article as:**
Pandey, D. "The Critical Role of Identity and Access Management in Modern Enterprise Security Frameworks." *Sarcouncil Journal of Engineering and Computer Sciences* 4.7 (2025): pp 1357-1365.





**Publisher: SARC Publisher**