Clareus Scientific Science and Engineering
Volume 2 Issue 10 December 2025
DOI: 10.70012/CSSE.02.061
ISSN: 3065-1182

Transitioning Legacy Infrastructure into a Future-ready IAM Environment that Enhances Scalability, Compliance, and Intelligence

Citation: Shreekant Rangrej. "Transitioning Legacy Infrastructure into a Future-ready IAM Environment that Enhances Scalability, Compliance, and Intelligence". Clareus Scientific Science and Engineering 2.10 (2025): 02-09.

Article Type: Review Article

Received: November 01, 2025

Published: November 09, 2025

Shreekant Rangrej*

SAP GRC and Security Architect, Cybersecurity Expert, USA

***Corresponding Author:** Shreekant Rangrej, SAP GRC and Security Architect, Cybersecurity Expert, USA.

Abstract

Legacy systems have provided the backbone for many organizations' digital operations for years, yet legacy systems lack the ability to be as agile to current cybersecurity challenges. Hybrid cloud environments, mobile workers, and increased sophistication of threat actors present challenges that legacy identity management technologies fail to provide adequate security and regulatory compliance. Organizations are looking for solutions that will evolve with the increasing challenges presented by the digital environment. This paper presents research focused on creating an identity ecosystem capable of adapting to future challenges which are to replace legacy identity management systems. The Identity and Access Management (IAM) system has scalable capabilities, is aligned with regulatory requirements, and includes built-in intelligence to identify and address cyber threats. The IAM system has capabilities such as multiple forms of advanced authentication, real-time monitoring and policy-based controls to ensure all users have secure access across all environments. This allows organizations to better manage their identities, protect sensitive information and respond quickly to potential threats. The overall result is to provide a robust, compliant and intelligent digital identity solution for organizations in a world of rapid change.

Keywords: Identity and Access Management (IAM); Legacy Infrastructure Modernization; Zero Trust Security; Cloud-Based IAM; Automation and Robotic Process Automation (RPA); Artificial Intelligence (AI) and Machine Learning (ML); Governance; Risk; and Compliance (GRC); Privileged Access Management (PAM); Multi-Factor Authentication (MFA); Decentralized Identity (DID) and Blockchain; Policy-Based Access Control (PBAC); Quantum-Resistant Security; Edge and IoT Integration; Identity Intelligence and Trust Scoring

Introduction

Organizations are struggling to keep up with the increasing demand of managing user identities, granting access to resources, and meeting regulatory requirements. The digital identity ecosystem is expanding rapidly, but traditional identity systems were designed for static on-premises environments with manual processes and fragmented data silos. Legacy infrastructure does not have the adaptability or intelligence needed to support the evolving threat landscape and hybrid IT environ-

ment.

There is no option to modernize legacy infrastructure — it is mandatory for organizations to be agile, innovative, and secure. At the center of this transformation is Identity and Access Management (IAM). A robust IAM framework will ensure that the correct users have access to the correct resources at the correct times while continually validating trust between systems.

This article will explore how organizations can transform legacy IAM systems into secure, intelligent, and future ready digital ecosystems. We will also discuss the key technologies, governance strategies, and emerging trends that will impact the modernization of IAM.

Understanding Legacy Infrastructure in IAM

Characteristics of Legacy Systems: Legacy IAM systems have characteristics including:

- Static user directories that do not synchronize well with other systems.
- Provisioning and de-provisioning of access rights are performed manually.
- Authentication methods are decentralized across various business applications.
- Integration with cloud platforms and APIs is weak or non-existent.
- Visibility into access patterns and risk exposures is limited.

Legacy IAM systems are often supported through aging technologies like LDAP directories or custom scripts that are difficult to maintain and scale. As organizations move workloads to the cloud or implement SaaS platforms, legacy IAM becomes a bottleneck and exposes gaps in access control and compliance.

Limitations and Risks

Outdated encryption protocols and insufficient patching expose systems to serious security vulnerabilities [1], while users often face inconsistent access experiences across on-premises and cloud environments. Regulatory compliance with standards such as GDPR, SOX, and HIPAA remains challenging, especially when identity and access management (IAM) processes are handled manually. This manual administration not only causes operational inefficiencies and delays in user onboarding but also contributes to a high Total Cost of Ownership (TCO) for legacy IAM systems, placing a strain on IT resources and budgets.

Reasons to Modernize Legacy environment to future-rich IAM

The need for modernization of IAM within legacy environments is driven by several factors:

1. ***Hybrid and Multi-Cloud Adoption***: Organizations are operating across a wide range of platforms – AWS, Azure, Google Cloud, and private data centers. Traditional IAM systems are unable to manage federated identities across such distributed environments [2].
2. ***Zero Trust and Evolving Security Models***: Zero Trust frameworks have changed the way access is controlled. Never trust; always verify. Therefore, continuous authentication, behavior analysis, and context-sensitive decision-making capabilities are necessary for Zero Trust frameworks. Such capabilities do not exist in legacy IAM.
3. ***Data Privacy and Compliance***: Transparency, least privilege enforcement, and auditable records of access activity are all required by regulatory mandates. Legacy IAM does not possess automation and reporting tools to meet these requirements efficiently.
4. ***Remote Access and the Digital Workforce***: With remote work becoming a permanent fixture, secure identity verification outside of the corporate perimeter is critical. Legacy VPNs and password-based systems are no longer adequate.

Modernization Strategies for IAM Ecosystems

Modernizing Identity & Access Management (IAM) is more than a simple technology update; it requires an organizational-wide strategic transition that requires an architectural redesign, automation and a cultural alignment in order to be successful. Typically,

the modernization process starts by rehosting, where current IAM systems such as legacy Active Directory, Identity Manager, etc., are migrated to cloud based platforms such as Microsoft's Azure AD, which provides for increased scalability, reliability and other features.

The next phase of modernization is refactoring, where containers, micro-services and APIs are used to create a modular IAM platform design that will allow for easy integration with modern applications and services [3]. As organizations continue to evolve, they typically begin to re-architect their IAM frameworks to include federation protocols (SAML, OIDC), continuous authentication, and Zero Trust concepts into their IAM architecture. By doing so, organizations position identity as the center of their enterprise security perimeter. Some organizations go through a full rebuild or replacement of their current IAM platforms using cloud native IAM platforms (Okta, Ping Identity, ForgeRock, etc.) to provide them with advanced analytics capabilities, automation capabilities, and the ability to adapt to changing security requirements.

Finally, as part of the modernization process, many organizations retire all obsolete systems, and redundant access modules to reduce complexity and decrease their attack surface. When combined, each of these phases provide assurance that IAM not only supports regulatory compliance, and operational efficiencies, but is also enhancing the organization's overall cybersecurity posture.

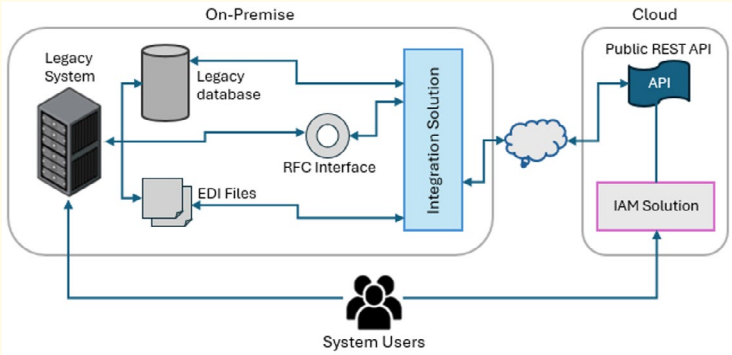

Figure 1: Legacy and modern infrastructure ecosystem.

Figure 1 demonstrates how legacy or on-premise systems can be seamlessly integrated with modern cloud-based IAM solutions to address regulatory compliance, improve operational efficiency, and strengthen the organization's overall cybersecurity posture.

Enablement Technologies

- ***Cloud-Based IAM***: The Cloud provides many benefits in terms of scalability, redundancy, and synchronization in real time [4]. Cloud IAM solutions also allow for a hybrid environment through federation, providing users with Single Sign-On (SSO) capabilities across all of their environments.
- ***Zero-Trust Security***: Modern IAM integrates with zero-trust models and validates every request based upon identity, device posture, and behavioral context instead of network boundaries.
- ***Automation and RPA***: Robotic Process Automation (RPA) enables automation of onboarding/offboarding, and automated review of access rights, which will enhance efficiency and reduce human error [5].
- ***Artificial Intelligence/Machine Learning***: AI/ML enhances the ability to identify threats to your organization through enhanced anomaly identification in user behavior, and detection of misuse of privileges and session hijacking [6].
- ***APIs and Microservices***: API-enabled IAM architectures create modular, scalable, and interoperable identity services across an organization's enterprise systems.
- ***Blockchain and Decentralized Identity (DID)***: Emerging technologies, including blockchain, introduce decentralized [7], us-

er-centric identity verification mechanisms, enhancing user privacy and control.

Security Foundations of a Modern IAM Ecosystem

In today's perimeter-less digital environment, all identities – whether they be human or machines – represent an opportunity for cyber threats. Because traditional network boundaries are eroding, Identity and Access Management (IAM), will need to evolve into the first line of defense against cyber threats. To achieve this, a solid IAM framework must be built using strong authentication, continuous monitoring, and policy-driven access control to limit which entities can interact with critical systems and/or data to only those who have been approved.

Multi-Factor Authentication (MFA) is also important to the IAM strategy because it verifies access through multiple layers of credentials [8]. Some examples of credentials used in MFA include biometric identification, token-based authentication, and contextual elements, including location, device type, etc. The use of MFA provides organizations with the opportunity to reduce the risk of their accounts being compromised and/or unauthorized access to an organization's systems and data.

Organizations must also incorporate Privileged Access Management (PAM) solutions to continue to build out the strength of their IAM frameworks [9]. PAM solutions protect high level administrative accounts from having the ability to provide unauthorized access by implementing just-in-time access, reducing the exposure time for high level accounts, and monitoring the activity of the privileged sessions for any signs of suspicious activity. The implementation of PAM solutions will help organizations minimize the risk of insider threats and misuse of high-level permission.

The integration of Security Information and Event Management (SIEM) systems with IAM will add additional layers of protection for organizations [10]. SIEM systems will monitor login activity, identify anomalies, and alert organizations to any unusual access attempts in real-time, allowing organizations to rapidly respond to incidents and mitigate threats.

Lastly, encrypting identity data stored and transmitted, both in motion and at rest, is necessary for organizations to maintain regulatory compliance and protect sensitive information [11]. Encrypting identity data will prevent unauthorized individuals from accessing encrypted data, regardless of how the data was accessed.

Together, the various IAM components discussed above will form a comprehensive security strategy that will allow organizations to adapt to modern threats, support organizational agility, and establish trust within digital environments.

Figure 2: Core Security Principles of a Modern IAM Ecosystem.

Figure 2 Illustrates, how a contemporary IAM system is based upon several core security principles; these include strong authentication, limiting privilege to the minimum required for access to perform an action, and real-time monitoring. Modern IAMs verify identities and limit access to sensitive data or applications using multi-factor authentication (MFA) and role-based, contextual, and risk-based access control models. Additionally, by utilizing analytics in real time and enforcing policy driven controls within an organization, only those who have been approved will be allowed to interact with sensitive data, reduce the organizations attack surface, and improve its compliance posture.

Governance, Risk & Compliance (GRC)

Modern IAM must operate seamlessly within established GRC frameworks to satisfy compliance obligations and maintain operational integrity.

Policy-Based Access Control (PBAC)

Access to organizational resources can be dynamically controlled through PBAC based on an individual's risk level, user behavior, and real-time context [12].

Regulatory Alignment

Modernizing your IAM will also align you with regulatory frameworks such as:

- GDPR for managing consent and privacy.
- SOX for financial access controls.
- ISO 27001 for information security governance.
- HIPAA for protecting health care related data.

Audit & Reporting

Automating audit trail reporting enables visibility to who has accessed what, when, and why, which will provide the foundation for both audit and forensic analysis.

Examples of Case Studies

Banking and Financial Sector

A well-known global bank overhauled its identity and access management (IAM) structure from old legacy LDAP directories to a state-of-the-art federated IAM solution thus enabling centralized authentication and decreasing user access to various systems. To improve security, the bank instituted multi-factor authentication (MFA) and employed advanced behavioral analytic techniques thus facilitating real-time visible knowledge of user activity and monitoring for anomalies. This move was not only beneficial in composing a stronger cyber-security posture but reduced unauthorized access by 45%. Also, the improved visibility and control of user access contributed to better audit preparations and regulatory compliance standards for the bank. This large-scale redo of its IAM systems has facilitated the bank's ability to become more resilient to and operationally efficient in its proactive management of risks arising from the constantly evolving threat landscape.

Health Care

A cloud-based Identity and Access Management (IAM) system that used role-based access controls and a Zero-Trust security model was implemented at an integrated hospital network. This contemporary system ensured that access to sensitive patient data was dynamically constrained by various contextual factors including user department and physical location as well as risk profile of the accessing device. By employing these dynamic controls, the organization was able to enhance data privacy and lower the risk of unauthorized access. The implementation also resulted in strengthened compliance with healthcare regulations as well as improved

operational efficiency by aligning access rights with ongoing risk assessments as well as organizational roles.

Manufacturing

An international manufacturer transformed its Identity and Access Management (IAM) system through integration with both Active Directory and Azure Active Directory. As a result, the firm was able to create federated identities in the cloud for easy access, as well as enable centralized access control. In addition to this integration, the firm developed an implementation of just-in-time (JIT) privileged user management. JIT allows users to have their privilege elevated temporarily as needed. The two major enhancements resulted in the reduction of administrative tasks by 60% for the firm, which resulted in streamlined access requests, and less reliance on manual interventions. In addition to the reduction of administrative burden, the improvements in IAM resulted in the firm's compliance capabilities being greatly enhanced due to the enforcement of the "least privilege" principle and the creation of detailed logs of all access activity. Overall, the IAM transformation provided significant improvements in security, operational efficiency, and adherence to regulatory compliance standards globally for the firm.

Strategic Framework for Modernizing Identity and Access Management

A well-defined roadmap is necessary to allow for a successful transition to an Intelligent IAM Ecosystem, as well as sustainable success:

Step 1: Assessments: Assess your current IAM capabilities [13]; identify the gaps and what IAM components are dependent upon each other; map legacy components to modern equivalent components.

Step 2: Define Strategy: Define your modernization strategy based on scalability, adopting Zero Trust, implementing automation, or meeting compliance requirements.

Step 3: Design Architecture: Design architecture based on modular and API driven architectures which support Hybrid Identity Management, as well as Dynamic Policy Enforcement.

Step 4: Implement: Implement new IAM components incrementally, i.e., cloud migration, SSO deployments, MFA rollouts.

Step 5: Optimize: Implement AI-driven monitoring, automated access review, as well as continuous improvement mechanisms.

Step 6: Train/Change Manage: Train users, administrators, and security teams on new IAM processes, tools, and compliance obligations.

Directions IAM Modernization Will Take

Identity Intelligence

Identity and Access Management (IAM) systems will use artificial intelligence (AI) to dynamically generate and update a user's or entity's "Trust Score" as they interact with different systems, applications and devices, transforming how we control who has access to our organization's most critical systems and data [14].

In this new dynamic IAM environment, the trust score would be based on both static factors such as roles, permissions and policies as well as dynamic factors such as user activity, location, time of day, type of device being used and other variables that could potentially indicate an increased level of risk for unauthorized access to a system or data.

This approach provides organizations with better, more timely insight into the potential threats to their network and allows them to make smarter, more informed, risk-based decisions about whether to grant access to a user or deny it. It also enhances security by providing ongoing evaluation of the behavior of the user and/or the devices being used prior to access is granted.

Password-less Authentication

Password-less authentication using biometrics and FIDO2 protocols reduces password-related risks associated with phishing and credential theft [15]. Password-less authentication enhances security by providing a means to verify the identity of a user through hardware-based authentication methods and therefore limiting the ability of unauthorized parties to gain access to the systems and data of a legitimate user.

Decentralized Identity

Decentralized Identifiers (DID's) utilize blockchain technology and provide end-users with complete control over their digital identities [16]. DID's are an improvement over existing digital identity systems because they do not require a centralized authority to authenticate the identity of a user, thereby reducing the number of single points of failure in these systems. DID's enhance privacy, security and resilience by empowering users to manage their own identity credentials independent of a particular platform, application or service. This enables users to establish trust in digital interactions and in decentralized ecosystems.

Quantum Resistant Security

As quantum computing continues to advance, Identity and Access Management (IAM) systems will have to adopt Post-Quantum Cryptographic Techniques to protect against quantum-based attacks on their digital assets [17]. These techniques will provide organizations with long-term protection against potential vulnerabilities in traditional encryption algorithms resulting from advancements in quantum computing.

Edge/IoT Integration

To support the expanding needs of IoT, Edge and Distributed Networks, IAM systems will have to evolve to provide scalable solutions that can securely provide access and perform large-scale identity verifications across billions of devices at the edge of the network [18]. The ability to provide resilient, context aware authentication to protect distributed networks and maintain performance and compliance in rapidly decentralizing digital environments will become essential to organizations seeking to implement and sustain a competitive advantage.

Obstacles and Considerations

- ***Interoperability***: Legacy Systems will need to be integrated with new IAM Solutions via Middleware, APIs and Connectors.
- ***Cost and Complexity***: Significant investments of time and money will be required to plan for IAM Modernization and minimize downtime and risk associated with migrating data.
- ***Cultural Resistance***: Automated IAM will often encounter Organizational Resistance due to the loss of manual control. Ongoing training and Executive Sponsorship are necessary to facilitate this process.
- ***Privacy/Ethics***: Governance and Ethical Oversight will be necessary to maintain a balance between the use of Automation, Analytics and User Privacy [19].

Conclusion

Legacy technology is being updated to include an intelligent and secure Identity and Access Management (IAM) system for many reasons. In addition to becoming a necessary element of business strategy as more businesses move to the cloud, use zero trust architectures and incorporate artificial intelligence; identity has become the foundation of digital trust. This will allow for ongoing verification of users and devices, and allow for flexible access to applications, services and data and allow for access from multiple platforms in hybrid environments, providing dynamic authentication of users and devices based on context and risk. The creation of a future ready IAM provides for greater than the protection of your business's assets and creates an environment for compliance, agility, and innovation.

Organizations that incorporate automation, intelligence, and governance into their IAM will be able to automate access to applications and services, decrease the time and resources required by IT staff to administer access to applications and services, increase transparency into how users interact with applications and services, and be better prepared for changing threats and regulatory requirements. Companies that act now will have the ability to proactively address the challenges and opportunities associated with creating a more secure digital economy. Investing in IAM today is more than protecting assets, it is also investing in the growth, trust, and transformation needed to thrive in a rapidly digitizing world.

References

1. National Security Agency. "NSA releases cybersecurity guide on detecting and fixing outdated encryption protocol implementations". Security Magazine (2021).
2. CDW. "Top 3 Reasons to Modernize Your IAM Program". CDW (2023).
3. Winayaka Ruhur. "Design and Security Evaluation of IAM Module in Microservice Architecture Using Keycloak". The Indonesian Journal of Computer Science 14.2 (2025).
4. Arun Ganapathi. "Architecting Cloud-Native I am: A Microservices-Based Approach to Modern Identity Management". International Journal of Computer Engineering and Technology (IJCET). 16.01 (2025).
5. Amro Al-Said Ahmad and Peter Andras. "Scalability analysis comparisons of cloud-based software services". Journal of Cloud Computing 8.10 (2019).
6. Biswanath Saha. "Robotic Process Automation (RPA) In Onboarding and Offboarding: Impact on Payroll Accuracy". ResearchGate (2024).
7. Purushottam Perapu. "Anomaly Detection in User Behaviour Using Machine Learning for Cloud Platforms". International Journal of Scientific Research in Computer Science, Engineering and Information Technology (2025).
8. Maria Polychronaki. "Decentralized Identity Management for Metaverse-Enhanced Education: A Literature Review". MDPI Electronics 13.19 (2024).
9. Samson Ojo and Allan covey. "Identity and Access Management (IAM) Authentication Methods: Importance of Multi-Factor Authentication (MFA) and Single Sign-On (SSO) and Access Control Models". Preprints.org (2025)
10. "Introduction to Privileged Access Management". ResearchGate (2024).
11. Mark Nicolett and Earl Perkins. "Apulse Technology". SIEM and IAM Technology Integration (2023).
12. Walid Rjaibi. "Holistic Database Encryption". SciTePress (2018).
13. IDPro Body of Knowledge (BOK) (2023).
14. Cloud Security Alliance (CSA). Modernization Strategies for Identity and Access Management (2024). https://cloudsecurityalliance.org/blog/2024/11/04/modernization-strategies-for-identity-and-access-management
15. Sateesh Kumar Nallamala. "AI-Augmented Identity and Access Management for Zero-Trust Architectures in Distributed Enterprises". American Journal of Data Science and Artificial Intelligence Innovations 3 (2023).
16. Manuel Barbosa., et al. "Provable Security Analysis of FIDO2". Cryptology ePrint Archive (2021).
17. Walid Fdhila., et al. "Methods for Decentralized Identities: Evaluation and Insights". Business Process Management: Blockchain and Robotic Process Automation Forum (2021).
18. Ana I González-Tablas and María Isabel González Vasco. "Quantum-resistant authentication: Securing identity and data against quantum threats". AIMS Mathematics 10.8 (2025): 17423-17458.
19. Kazi Masum Sadique, Rahim Rahmani and Paul Johannesson. "DIdM-EIoTD: Distributed Identity Management for Edge Internet of Things (IoT) Devices". Sensors 23.8 (2023): 4046.
20. NASSCOM Community. IAM Challenges in the Modern Enterprise (2021). https://community.nasscom.in/communities/cyber-security-privacy/iam-challenges-modern-enterprise