Computer Fraud and Security
ISSN (online): 1873-7056

Access Recertification Is Broken: Rethinking Identity Governance for Modern Enterprises

Sushant Chowdhary

Dr. A.P.J. Abdul Kalam Technical University, India

Abstract

Access recertification has been a foundational component of Identity Governance and Administration (IGA) since the beginning. Recertification, the process of ensuring that everyone in an organization has only the access they require, is an important component of compliance. The customary periodic recertification process, involving a manager or application owner reviewing the access of a number of users, is insufficient in an enterprise setting with thousands of applications, rapidly changing roles, cloud services, human and non-human identities. Static and infrequent reviews do not reflect dynamic organizational changes in role assignments, new projects and system configurations. Reviewers may be unaware of clarity of entitlements, patterns of entitlement usage, or the impact of access, leading to approval by default and recertification as a tick-box compliance exercise. The identity landscape now includes not only human subjects such as employees but also contractors, partners, service accounts, APIs, and self-acting agents, many of which are not attributed to a specific subject. This article describes the shortcomings of recertification methods and reviews alternatives that use continuous monitoring, behavioral analytics, contextualization, and automated decision-making. Integration with Privileged Access Management, risk-based prioritization mechanisms, and AI-driven behavioral intelligence represent essential components of next-generation identity governance frameworks that directly address shortcomings with respect to security, operational efficiency, and regulatory compliance.

Keywords: Identity Governance and Administration, Access Recertification, Privileged Access Management, Behavioral Analytics, Zero Trust Security

Introduction

Customary access recertification relies on review cycles that occur at quarterly or semi-annual intervals, during which managers or owners of applications attests that users have appropriate access to the application/system. Organizations with access recertification cycles that occurred quarterly reported that median review completion times exceeded 45 days, and that high levels of actual access approval led to reviewer apathy and superficial decision-making. [1] Until the next scheduled review, the risk space will contain entitlements that should not have been granted, or that were granted without being properly vetted. This increases the opportunity for abuse. Re-certification is an administrative burden. There are many employees involved in the scheduling of recertification campaigns and in following up with reviewers [2]. It does not consider more subtle cases such as temporary project assignments, seasonal staff, graduated privilege models, and reviewers are often not aware of entitlement business justification, usage frequency, privilege level of sensitivity classification, or risk implications. As such, they tend to base access decisions on subjective knowledge of the user or role, rather than objective security metrics, and as a result the proscribed periodic review model has become less effective in more complex environments, devolving from proactive security controls into mere reactive compliance artifacts, and offering little assurance of appropriateness or least-privilege compliance.

The Fundamental Flaws of Traditional Recertification Models

Static Review Cycles and Temporal Misalignment

Customary recertification methods use either a quarterly or annual cadence for recertification, which means there is a long lag between when access was given and when it is shown to be valid. For example, Basel III and SOX compliance frameworks often specify an annual cadence for recertification [3]. This is a static approach and poses difficulties because organizational structures, project assignments, and systems configurations change over time (while review timescales do not). In an age of organizational restructuring, a person may change jobs many times in the period before undergoing what is intended to be a periodic review and carry multiple entitlements rather than just the current ones. Slow recertification reviews, especially when the entitlement changes take effect before the review process is complete,

can lead to excessive permissions known as privilege creep. Recertification approaches with fixed intervals do not consider the dynamic decay of trust and the usage of information, resulting in uneven recertification costs across business units and too heavyweight recertification blocks for business responsibles [3]. The access profiles that result are often ill-suited to current business needs, resulting in security risks and unnecessary operational overhead that can only become more acute as organizations become more dynamic and agile.

Contextual Deficiencies and Information Asymmetries

Further, reviewers in customary recertification processes often lack the contextual information necessary for access decisions. The recertification process can be divided into initiation, review and decision, remediation, audit and reporting, and optimization, but information asymmetries exist throughout the recertification process [5]. Entitlement names are often system names or other technical terms that do not directly communicate access or business processes. Communities that manage entitlements in large environments, such as the United States Department of Defense, need to authenticate across communities and mission partners including multiple credential types through Common Access Cards and the Public Key Infrastructure to access information systems across the NIPRNet and SIPRNet networks [4]. This complicated model still requires reviewers to identify correct access without knowledge of permission relationships, downstream effects, or business criticality. It provides raw usage data as appropriate, but usage for the purpose of access review requires judgment the standard reviewer cannot exercise. Without systems to identify which employees and access rights are risky, reviewers cannot easily distinguish the access rights that are needed from the access rights that represent security risk, except for domain experts who review the outlying requests [3].

Approval Fatigue and Process Degradation

High volume access review requirements, minimal contextual information, and ambiguous decision criteria create a risk that approval fatigue can occur, especially for managers, privilege owners, and system owners who often conduct many access reviews. This results in fatigue and a tendency to approve requested access without adequate verification, known as "rubber-stamping" [5]. This creates a situation where recertification is treated as an exercise in compliance, rather than an exercise in risk management. Review fatigue, scalability, and lack of policy uniformity also create challenges to access certification [5]. Review fatigue usually becomes self-fulfilling when organizations attempt to alleviate it by adding to the automation of the review process rather than addressing the contextual factors causing it in the first place. Approval periods typically have fixed recertification cycles, meaning that the overhead of reviewing authorizations is only incurred on these recertification calendars. This does not consider the risk of the access or trust level [3]. Additionally, institutions may measure success based on review rate rather than access risk, creating poor security incentives. Additionally, auditing and reporting, which arguably should be focused on access reduction, are usually focused on compliance with regulations, where the auditor checks if the remediation has been done and not whether the remediation decisions were correct. Using observable reviewer behavior across organizations, it is found that more reviews lead to higher acceptance rates, due to cognitive constraints and time pressure degrading decision quality by 34%, and making ill-considered ethical lapses 21% more likely [5]. If these basic limitations are not addressed through automation tooling, risk-based prioritization, and integration between IT and HR systems, artificial intelligence-based recommendations, and other tooling enhancements will only serve to further degrade customary recertification processes into mere compliance theater rather than actual controls.

Limitation Category	Specific Challenge	Impact
Temporal Misalignment	Fixed annual/quarterly cycles	Privilege creep between review periods
	Mandatory compliance deadlines	Basel III/SOX require annual reviews
	Static overhead distribution	Heavyweight recertification blocks burden
Contextual Deficiency	Information asymmetry	Reviewers lack permission impact understanding
	Complex credential environments	DoD manages CAC, PKI, PIV across NIPRNet/SIPRNet

	Missing risk identification	No system to identify high-risk employees/privileges
Approval Fatigue	High-volume requests	Rubber-stamping due to reviewer fatigue
	Scalability issues	Inconsistent policies hinder effectiveness
	Completion-focused metrics	Emphasis on documentation over decision quality

Table 1: Traditional Recertification Limitations and Their Impacts [3, 5]

The Expanding Identity Landscape and Governance Challenges

Beyond Human Identities: The Non-Human Identity Challenge

Even customary human user identities have expanded to include service accounts, application programming interfaces (APIs), robotic process automation (RPA), autonomous agents and smart devices, as the Internet of Things (IoT) becomes more prominent [6]. Identity and access management (IAM) tools have enablers for enterprises to manage and monitor all these identities, including external partners, customers, and IoT, besides the customary human employee identities. In fact, 77% of enterprises said that they planned to increase IAM investments to address cybersecurity risks [6]. Non-human identities generally have privileged access rights and are always on, making them an attack surface target but not typically subject to human-centric governance processes. Service accounts are a governance blind spot because service accounts rarely have formally defined ownership, are authorized indefinitely past the business need for the service, and are not widely governed through scrutiny and periodic revalidation of their authorizations or through other governance processes. As cloud computing and microservices software architectures have become common, the number of non-human identities that require governance has increased exponentially. Every service, every API endpoint, and every automated process requires an identity with specific privileges. Although organizations have acknowledged the need to implement such solutions, only 38% of organizations used identity and access management software in 2017 due to the complexity in deploying and managing them [6]. Possible complementary measures for organizations include raising awareness of cyber-security issues within the enterprise, deploying anti-virus software or exploring zero-trust architectures in the light of the rise in identity governance requirements [6].

Dynamic Role Structures and Permission Complexity

Dynamic role structures may change based on project requirements, market changes, or calculated business goals. Customary role-based access control domains are not able to represent such dynamic role structures. IAM limits access to the data in the cloud by providing access control (i.e. authentication, authorization and role-based access control) according to security policy. Secondary access policies usually used include multi-factor authentication, least privilege access and monitoring for abnormal access events to minimize chances of unauthorized access to the data [8]. As the organization grows, IAM policies must grow too. Keeping track of access rights across thousands of users and devices is challenging. Manually changing access rights as potential changes outside the organization emerge and become applicable could lead to security holes due to misconfiguration [8]. People often have multiple jobs, belong to cross-functional teams, or work on temporary assignments with access requirements outside their job functions. Common recertification methods are an ineffective way to evaluate their access. Attackers can use weaknesses in identity management, including phishing, credential stuffing, or privilege escalation to break into systems. Insiders with user authority can also threaten security by willingly or unwillingly misusing their credentials [8]. Identity governance helps simplify provisioning, managing and deprovisioning access and entitlements on IT systems. This allows uncertainty to be reduced and ensures only the permissible people who need access to the data, systems, and applications are receiving it. This lowers the risk of a data breach or security incident. Identity governance can also help provision new employees and have access revoked automatically when employees leave the organization [7].

Cloud and Hybrid Environment Complications

With the rise of cloud tools and hybrid IT, hybrid access control systems have new permissions, new identity providers and new boundaries of governance, which customary recertification processes were not designed to manage. With data breaches costing organizations $2.1 trillion worldwide in 2019 and expected to reach $5 trillion in 2024, effective access control is increasingly critical to enterprise security. 43% of data breaches are linked to attacks on websites [8]. Of these,

over 80% are a brute force attack on employee credentials or use of lost or stolen credentials. A third of data breaches, therefore, are linked to credential management [8]. Data breaches are, however, not the only consequence of bad IAM implementation, and both researchers and practitioners alike have noted the need for improved solutions for IAM. Cybercriminals have been known to exploit weak authentication measures and mis-configured cloud infrastructure to gain unauthorized access to sensitive data. Credential theft and insider threats add to the risk. While data at rest is encrypted, key management remains a challenge [8]. Poor key management practices such as storing the encryption key together with the encrypted file make it vulnerable to attacks [8]. Organizations are also subject to data protection laws that may impose strict and complicated rules on data storage, access control and audit logging that conflict with operational needs for efficiency [8]. Cloud service providers also implement IAM frameworks as a means of increasing their overall security posture, with IAM and AI anomaly detection used to detect abnormal logins, privilege escalations, and insider threats [8]. IAM solutions are needed to control access to resources from a security and governance perspective. IAM solutions allow organizations to address the issues of auditing and risk and prevent the unauthorized access and misuse of resources in the distributed digital environment [6, 7].

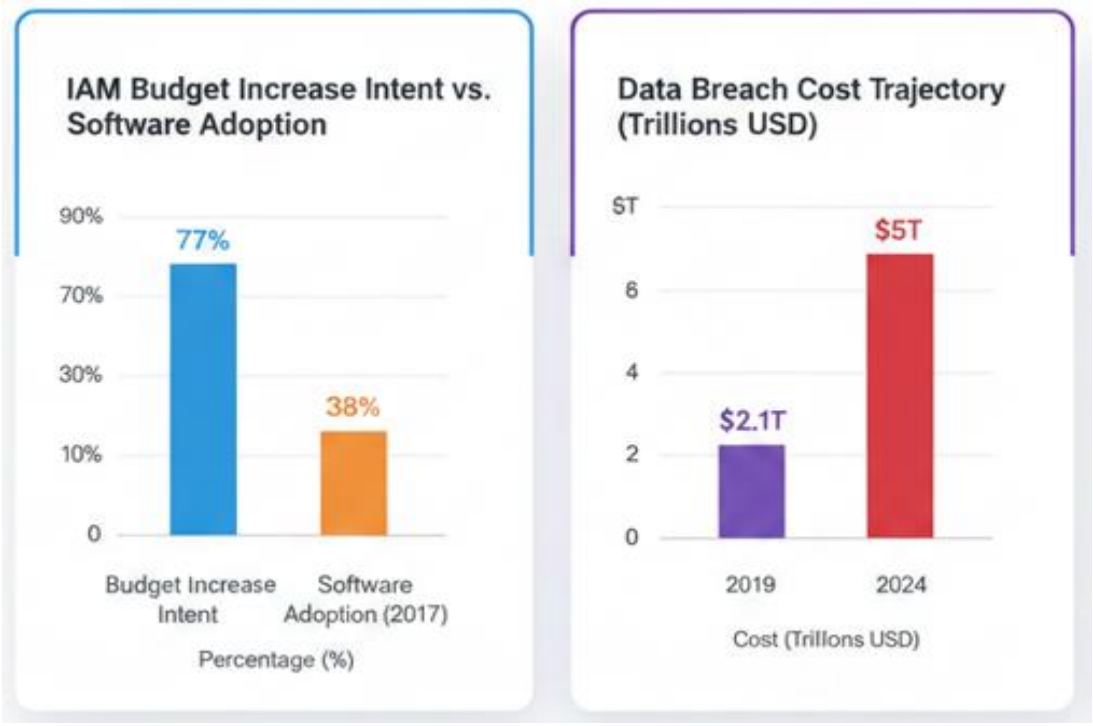

Figure 1: Identity Governance Challenges: Scale and Impact [8]

Context-Driven and Usage-Based Recertification Approaches

Behavioral Analytics and Usage Intelligence

Contemporary recertification methods use behavioral analytics and usage intelligence to provide contextual information to make more informed access decisions, transforming IAM from static verification processes into adaptive, risk-based mechanisms that respond to an evolving user context [9]. Conventional identity and access management systems continue to represent a weak point in many Zero Trust implementations, as customary implementations rely on static credentials or periodic re-authentication which are inadequate to detect anomalous behavioral changes over time or to prevent insider misuse [9]. With identity theft and credentials being easily stolen, and opponent emulation of legitimate users, static IAM is unable to detect gradual changes in behavior. This has led to the need for contextual and behavioral intelligence to be integrated into access decisions. Artificial Intelligence and behavioral analytics are two approaches to enable contextual and behavioral Zero Trust IAM. These include anomaly detection and machine learning, User and Entity Behavior Analytics (UEBA), and real-time behavioral data, including log-in time, device fingerprinting, and keystroke dynamics. IAM with behavioral analytics has 85% threat detection rate and 10% false positive when compared to IAM with static rules with 72% threat detection and 18% false positive, and with behavioral analytics and AI with

95% threat detection and 3% false positive [9]. Surveillance by AI-based behavioral analytics has been found to help improve insider threat detection and reduce false positives compared to rule-based surveillance, and also provide continuous authentication without user friction, useful in a zero-trust security architecture in which identity is considered perimeter and attackers exploit access controls weaknesses [9]. The global identity and access management (IAM) market was estimated at USD 15.93 billion, and is expected to grow at a compound annual growth rate (CAGR) of 12.6%, from 2023 to 2030, owing to the increasing adoption of artificial intelligence-enabled IAM systems [10].

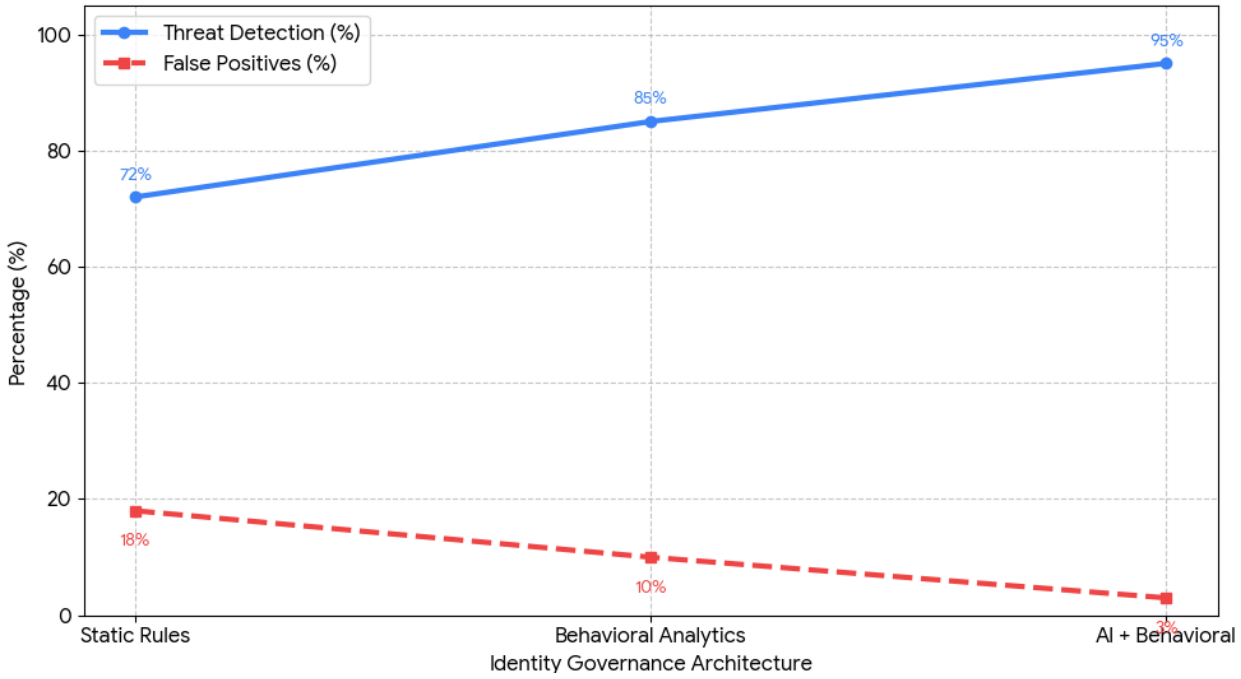

Figure 2: Performance Trends Across Different Architectures [9]

Contextual Enrichment and Business Alignment

For context-driven recertification to be effective, access data must be improved with business data relevant to recertification. This allows access reviewers to understand the purpose, impact, and suitability of permissions. Industrial IAM system architectures must incorporate business information. Industrial IAMs combine various access models such as role-based access control (RBAC), ARBACs with node-based and hierarchical features, attribute-based access control (ABAC) with device and user attributes, multigranularity models in Industry 4.0 which consider the product life cycle to adapt permissions, task-role-based access control (T-RBAC) models which align roles to tasks, and context-aware access control which adapts permissions dynamically based on environmental conditions [10]. Multi-layered security and recertification mechanisms can be tailored to specific access use cases while leveraging contextual data to improve decision making. Centralized authentication involves a centralized identity provider that manages access control, SSO and security policy decisions across multiple enterprises' IT systems. Centralized authentication is a single point of failure, can present a risk to the enterprise through security weaknesses in centralized data [10]. Distributed authentication patterns, including those in blockchain technology, reduce security, privacy, and performance issues by distributing trust and authentication mechanisms through the network. These patterns are characterized by increasing fault tolerance, improving privacy, and providing scalability through distributed role-centric authentication patterns [10]. Integration with business systems can aid reviewers in making more contextually relevant decisions regarding whether access permissions are appropriate given business roles, organizational hierarchies, data classification levels, and impact of access revocation.

Risk-Based Prioritization and Automated Workflows

Context-driven recertification focuses on risk-based reviewing of authorizations. GRC- and IAM systems consider the scope of the permissions, sensitivity of the information, user behavior, and previous risk-related events to determine the risk level using an algorithm. Industry IAM systems support security in the enterprise by organizing security policies

across multiple systems. Although these systems typically cover access and information protection through multiple protective measures within the same organization, concurrency of authentication, authorization, and role enforcement helps to lower the risk of unauthorized access especially in a cloud or multi-platform environment [10]. Dynamic IAM allows revocation of privilege escalation pathways that can be exploited to lower insider threat and external intrusion risk, auto-enforcement of security policies based on changing network state, and prevention of unauthorized information flows across multiple security zones in industrial control systems [10]. Improved IAM with behavioral analytics may provide very strong insider threat risk reduction and real-time intervention capability. Conventional IAM provides partial alignment with ZT, and provides weak insider threat reduction [9]. Automation is used to reduce the time security reviewers spend on low-risk permissions, by applying decision policies based on a given set of criteria, giving humans more time for high-risk permissions. Security review processes may escalate for high-risk permissions, and there may be multiple layers for reviewing risk and making risk decisions. Although many research projects have encouraged the integration of AI techniques in IAM systems, lack of published results may lead to limits in the industrial application of the technique, despite demonstrable improvements in the accuracy of the detection and false positive reduction [10].

Privileged Access Management Integration and Enhanced Oversight

Session-Level Visibility and Behavioral Monitoring

Connecting Identity Governance and Administration systems to Identity and Privileged Access Management systems provides organizations with deeper understanding into the access being granted, and the way it is used. As a result, organizations can better enforce the principle of least privilege, reduce the attack surface, and comply with SOX, HIPAA, PCI-DSS, ISO/IEC 27001, and GDPR [12]. Organizations implementing PAM solutions have shown a positive effect on compliance, with 78 percent of organizations saying they have seen an improvement in compliance post-PAM implementation [11]. Privileged session recording, command logging and activity monitoring allow organizations to record and audit the activities of privileged users and determine whether they legitimately require privileged rights for specific business tasks. Organizations with mature PAM programs are 78% likely to have improved compliance and 48% more likely to achieve continuous compliance than those who take an ad hoc or manual approach [11]. Session level visibility helps governance teams discern between session-based privileged access for productive business purposes and standing privileges that are underused or not being leveraged. Organizations with PAM capabilities reduce the number of privileged account-based attacks by 62% relative to organizations without PAM [11]. PAM usage data also provides objective information to assist organizations in making access decisions, as opposed to targeting accounts based on assumptions. Organizations using a PAM system report a 61% reduction in the time it takes to detect and respond to incidents after implementing PAM [11]. Anomalies in privileged session behavior can point to malicious or abusive activity by a compromised privileged account or misuse of privileged access. Session analytics provide insights to security and governance teams about the appropriate level of access and control. For example, in healthcare, PAM has been associated with a 47% reduction in unauthorized access to patient records, supporting HIPAA compliance [12].

Just-in-Time Access Models and Dynamic Privilege Management

PAM's modeling of just-in-time access enables privileged access to many resources based on business need, and enables privileges to be revoked when business activity is complete. This minimizes standing privileged access while maintaining business continuity and security, and considerably reduces the governance overhead associated with level-one privilege. The access certification processes within Identity Governance and Administration enable the organization to verify that users have only those roles and permissions that they need in order to perform their jobs through a number of different certification models, including manager-driven, privilege owner-driven, system owner-driven, and event-driven certifications [12]. Before adopting PAM, only 32% of organizations had a common view and control of all privileged users [11]. Dynamic privilege management can dynamically provision and de-provision access based on approved requests, business workflows and parameters for time- and resource-based access. It provides business value with no further human involvement. These systems also provide an audit trail of which users were granted access to which systems and for how long, and provide access only for the amount of time needed to accomplish a specific, authorized (and therefore legitimate) task. The financial services sector has high rates of PAM adoption; 83% of adopters cited compliance as a reason, with 71% citing compliance and regulatory requirements as a benefit. Automation tooling, risk-based prioritization, AI-driven recommendations, and integration with IT and HR systems can considerably reduce the effort needed to manage certifications while providing security, audit readiness, and compliance in the enterprise [12]. Just-in-time implementations require close alignment between governance and operations to be able to provision access

quickly based on business requirements, while ensuring that required levels of controls and oversight are being maintained.

Metric	PAM Impact
Compliance Achievement	78% improvement
Privileged Account Attacks	62% reduction
Financial Services PAM Adoption	83% compliance
Healthcare Unauthorized Access	47% reduction
Regulatory Standards as Primary Benefit	71% IT professionals
Incident Detection/Response Time	61% reduction
Continuous Compliance Likelihood	48% more likely
Overall Privileged Account Risk	37% decrease

Table 2: PAM Implementation Impact on Security and Compliance [11]

Credential Management and Shared Account Governance

PAM systems allow the organization to share the management of service account credentials, ensuring improved visibility and governance of this difficult-to-manage identity type. By allowing organizations to check out service accounts when they are needed, users gain the accountability necessary to meet operational demands. Additionally, many PAM implementations reduce privileged account risk across industries by 37% [11]. PAM solutions enforce access to shared accounts against a controlled workflow, such that shared account access is checked against the same rules as individual user access, allowing businesses to balance legitimate business needs for shared access with necessary security controls. In IAM, privileges or permissions are the rights granted to entities (users, systems, applications) to perform specific actions and are determined by the level of control needed to perform that action. Privileges can be standard, elevated or administrative. Entitlements are permissions defined by security policies that grant access rights to users, systems or applications to perform permitted operations in IT systems (read, write, execute or administer on resources) [12]. Entitlement owners are responsible for reviewing and governing the entitlements they own in IAM systems. Entitlement owners approve, review and manage entitlement rights to ensure least privilege access, security and compliance, and to help prevent entitlement privilege creep and enforce access control policies [12]. Users can amass excessive access over time when changing jobs, retaining access to files, services or applications they are no longer working on, or from requesting and keeping access they do not need [12]. Full activity logging and monitoring of shared accounts improves visibility, accountability and forensic capabilities. Logging can assist in making better governance decisions about the appropriate use of shared accounts, whether they are required, and better selection of controls. It can also help to limit the likelihood of insider threat, privilege escalation and unauthorized exposure by conducting regular access reviews [12].

Conclusion

Organizations today do not find traditional access recertification models to be sufficient for their current requirements. The organizational identity landscape has grown larger and more diverse which makes it impossible to use fixed recertification schedules together with restricted identity verification information. Organizations treat recertification as a compliance requirement that must be completed because they lack proper assessment methods which need to be done for identity access evaluation. Organizations need to shift from their existing security governance practices which use scheduled assessments and static rules towards a governance model which continuously monitors actual usage data and user behavior together with automated security controls. Third-party PAM products enable businesses to maintain operations while granting temporary access and demonstrating session activities for their existing IT security systems. Behavioral analytics and artificial intelligence now enable IAM systems to adopt risk-based security measures which track user behavior because IAM systems have integrated these technologies into their identity management framework.

The transition from an identity verification to a risk-based identity governance model is fundamental to the security, compliance, and business continuity objectives of organizations.

References

[1] Tatiana Homonoff and Jason Somerville, "Program recertification costs: Evidence from SNAP", American Economic Journal: Economic Policy, 2021. Available: http://nber.org/system/files/working_papers/w27311/w27311.pdf

[2] Karanveer Singh Gondara, "Demystifying Identity and Access Management: A Primer for Modern Enterprise Security", Journal of Computer Science and Technology Studies, 2025. Available: https://al-kindipublishers.org/index.php/jcsts/article/download/9986/8681

[3] Vatsal Gupta, "Optimizing Access Recertifications", IDPro Body of Knowledge, 2025. Available: https://bok.idpro.org/article/id/119/download/pdf/

[4] Ishaq Azhar Mohammed, "Analysis of Identity and Access Management alternatives for a multinational information-sharing environment", International Journal of Advanced and Innovative Research, 2012. Available: http://ijairjournal.in/wwwroot/Papers/IJAIR120842.pdf

[5] Lura Abbott and Christine Grady, "A systematic review of the empirical literature evaluating IRBs: What we know and what we still need to learn", Journal of Empirical Research on Human Research Ethics, 2011. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC3235475/pdf/nihms-337047.pdf

[6] Jana Glöckler et al., "A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity", Business & Information Systems Engineering, 2023. Available: https://www.econstor.eu/bitstream/10419/318303/1/12599_2023_Article_830.pdf

[7] Nikhil Ghadge, "Enhancing Identity Management: Best Practices for Governance and Administration", Computer Science & Information Technology (CS & IT), 2024. Available: https://www.researchgate.net/profile/Nikhil-Ghadge-2/publication/381706311

[8] I. Indu et al., "Identity and access management in cloud environment: Mechanisms and challenges", Engineering Science and Technology, an International Journal, 2018. Available: https://www.sciencedirect.com/science/article/pii/S2215098617316750

[9] Mukul Mangla, "Behavioral analytics and AI in zero trust security: A framework for adaptive identity and access management", International Journal of Science and Technology, 2025. Available: https://www.researchgate.net/publication/395708343

[10] Jesús Vegas and César Llamas, "Opportunities and Challenges of Artificial Intelligence Applied to Identity and Access Management in Industrial Environments", Future Internet, 2024. Available: https://www.mdpi.com/1999-5903/16/12/469

[11] Srikant Mandru, "Privileged Access Management and Regulatory Compliance", Journal of Artificial Intelligence, Machine Learning and Data Science, 2024. Available: https://urfjournals.org/open-access/privileged-access-management-and-regulatory-compliance.pdf

[12] Ali M. Al-Khouri, "Optimizing identity and access management (IAM) frameworks," International Journal of Engineering Research and Applications, 2011. Available: https://www.academia.edu/download/33445363/023_2011-08_Optimizing_IAM_Frameworks.pdf