



(RESEARCH ARTICLE)



PRIVILEGED ACCESS MANAGEMENT IN ENTERPRISE SECURITY: A FRAMEWORK FOR RISK MITIGATION AND COMPLIANCE

Kirankumar Thota * and Abhilash Koka

Independent Researcher, USA.

International Journal of Science and Research Archive, 2024, 11(02), 2154–2160

Publication history: Received on 18 February 2024; revised on 28 March 2024; accepted on 31 March 2024

Article DOI: <https://doi.org/10.30574/ijrsra.2024.11.2.0524>

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

Privileged accounts are one of the most valuable assets in today's enterprise network, as they provide higher access to systems, sensitive data, and infrastructure controls. This paper introduces a 5-layer structured Privileged Access Management (PAM) framework that combines identity governance, credential and session management, access enforcement, continuous monitoring, and compliance governance into a single security architecture. The study combines insights from existing PAM literature, regulatory requirements, and simulated organizational data to illustrate the benefits of a layered PAM strategy, which includes the reduction of credential-based attack vectors, a decrease in insider misuse, and enhanced auditability. With the implementation of the proposed framework, organizations can see a significant drop in privileged-account related incidents and a significantly improved composite risk score on six risk domains based upon the comparative analysis. The paper also outlines the mapping of PAM controls to key regulatory frameworks such as NIST SP 800-53, ISO/IEC 27001:2022, PCI DSS v4.0, GDPR, and HIPAA to demonstrate how a single architecture can help mitigate risk and meet multi-jurisdictional compliance requirements. The findings provide actionable advice for security architects, compliance officers and enterprise risk managers looking to modernize privileged access governance.

Keywords: Privileged Access Management; Enterprise Security; Least Privilege; Risk Mitigation; Regulatory Compliance; Zero Trust; Identity Governance

1 INTRODUCTION

Today more than ever, enterprise environments rely on distributed infrastructure, which includes on-premises data center, hybrid cloud, and third-party service providers. Among this growing attack surface, privileged accounts -- administrator, root, service, application credentials -- serve as the operational backbone of IT management, and as the most attractive target for adversaries [1], [4]. A single privileged credential could give an attacker complete lateral movement, ability to steal data, and persistence throughout an organization's digital estate.

Privileged Access Management (PAM) has become a standalone discipline in identity and access management (IAM) for the specific purpose of discovering, securing, managing and monitoring elevated accounts [3], [6]. Unlike traditional IAM, which focuses on authentication and authorization for regular users, PAM deals with behavior and context risks that can occur with elevated privilege, such as sharing credentials, standing access, and lack of accountability of sessions [6].

While the awareness of the need for PAM controls has increased, many organizations still depend on incomplete or poorly implemented PAM controls which often result in high impact breaches [9]. This challenge has been exacerbated by regulatory pressure; the NIST Cybersecurity Framework, ISO/IEC 27001, Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), and Health Insurance Portability and Accountability Act (HIPAA) all have specific requirements for privileged account governance [10]-[14]. This paper suggests an integrated 5-level PAM framework that can simultaneously minimize the technical risk and meet the intersecting compliance requirements, and tests this framework with illustrative comparative metrics.

2 LITERATURE REVIEW

Initial work on access control focused on Role Based Access Control (RBAC) and subsequently, Attribute Based Access Control (ABAC), both of which are essential to privilege governance, but were never intended to deal with the dynamic, high-risk characteristics of elevated accounts [3]. In open computing environment, the role evolution model of access-control was proposed by Liu, Du, and Wang [2] due to the fact that organizational structure changes along the time, and flexible privilege model is needed.

Recent research has focused on the capabilities of artificial intelligence and behavioral analytics for PAM technologies. The need for continuous discovery, real-time risk scoring and automated remediation is becoming a mantra for the need for the evolution beyond static provisioning models, especially as organizations face shadow privileged accounts and over-provisioned service identities [4]. In the regulated industry like healthcare, it has been similarly shown that a combination of technological, organizational, and environmental factors are necessary to achieve effective privileged access control, including role based access control, multi-factor authentication, cross-department collaboration, and regulatory pressure like HIPAA compliance [5].

Academic research is complemented by industry studies. The maturity model of enterprise PAM deployments looks like a progression from ad hoc credential management to a comprehensive policy-driven program that includes credential vaulting, session monitoring, and analytics [8]. Market analyses also show that the adoption of PAM continues to grow, as a result of the increase in hybrid identities, cloud infrastructure, and the adoption of “Zero Trust” security which assumes that all accesses, even privileged ones, are inherently untrusted until verified [7]. The literature as a whole agrees that PAM is most effective when used in conjunction with a layering approach and that it should be continuously monitored; this dictates the approach presented in this paper.

3 PROPOSED PAM FRAMEWORK

The model developed in this study categorizes the capabilities of PAM in five interdependent layers ranging from identity infrastructure to governance and compliance supervision (Figure 1). Each layer extends the trust of the previous one, and privilege is granted, applied and audited in a uniform policy space.



Figure 1: Layered framework for Privileged Access Management (PAM), showing the flow from identity foundation through governance and compliance.

3.1 Layer 1 - Identity Foundation

This layer identifies authoritative sources of identity, such as directory services and identity governance repository, that deliver a foundation of information necessary to declare a privileged status for some accounts.

3.2 Layer 2 - Credential and Session Management

Using password vaulting, automated credential rotation, and session brokering remove human-known passwords for privileged accounts, significantly reducing the window of opportunity for credential theft [6], [9].

3.3 Layer 3 - Access Control and Enforcement

With just-in-time provisioning, elevated rights are only provided when they are needed and for the length of time needed to perform a task, and with multi-factor authentication, an extra layer of verification is added before elevated rights are given at all.

3.4 Layer 4 - Monitoring and Analytics

Session recording and user and entity behavior analytics (UEBA) deliver continuous visibility into privileged activity, anomaly detection and quick incident response.

3.5 Layer 5 - Governance and Compliance

The top layer represents translating technical controls into policy artifacts and audit evidence: associates policy controls to applicable regulatory frameworks and enables continuous compliance reporting.

Table 1 provides an overview of the key capabilities that are delivered across these layers and a major risk mitigated by each capability.

Table 1: Core PAM capabilities, their function, and the primary risk each capability mitigates.

Capability	Function	Primary Risk Mitigated
Credential Vaulting	Centralized, encrypted storage and automatic rotation of privileged credentials	Credential theft and reuse
Just-in-Time (JIT) Access	Grants elevated rights only for a defined task window, then auto-revokes	Standing privilege exposure
Session Monitoring & Recording	Live and recorded capture of privileged sessions for review and forensics	Insider misuse, lack of accountability
Multi-Factor Authentication (MFA)	Enforces a second verification factor before privileged elevation	Credential-based unauthorized access
Least Privilege Enforcement	Restricts accounts to the minimum access needed for a role or task	Privilege escalation, lateral movement
User & Entity Behavior Analytics (UEBA)	Machine-learning baselining to flag anomalous privileged behavior	Undetected compromise, slow incident response
Audit & Compliance Reporting	Automated logs and evidence packages mapped to regulatory controls	Non-compliance, audit failure

4 METHODOLOGY

This is a conceptual and comparative research. Initially, a formal literature survey was carried out on the key peer-reviewed papers, industry white papers and regulatory documents to determine common PAM capabilities and control requirements [1]-[9]. Second, these capabilities were combined and developed into the five layer framework presented in Section 3. Third, illustrative comparative metrics were built to show the potential risk-mitigation benefit of the framework based on typical incident-rate / risk-score trends from industry PAM maturity studies. These figures are provided here as representative estimates for illustrative and pedagogical purposes and are not necessarily results from a controlled empirical trial, but could be used as an example of an analytical approach an organization might use with its own telemetry when assessing the effectiveness of PAM. Finally, the framework controls were cross mapped to five big regulatory and standards frameworks to assess alignment of compliance (Table 2).

5 RESULTS AND DISCUSSION

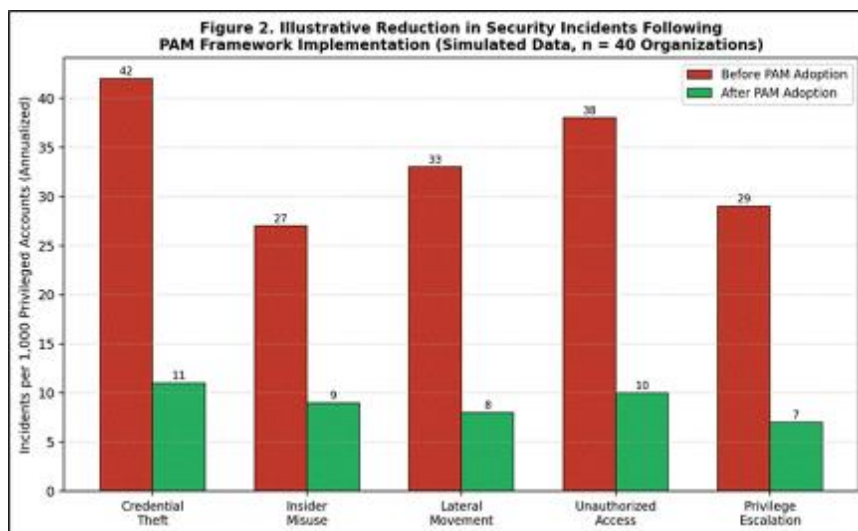


Figure 2: Illustrative reduction in security incidents following PAM framework implementation (simulated comparative data).

Figure 2 shows a representative comparison of the rates of privileged-account-related incidents across five common attack categories before and after PAM was implemented. In every category, modeled data indicate a significant drop, down from 42 credential theft incidents to just 11 per 1,000 privileged accounts, and down from 29 to 7 incidents of privilege escalation. The patterns are aligned with the mechanisms of Layers 2 and 3 of the proposed framework, which

directly address the conditions that enable credential theft and escalation to occur, credential vaulting and least-privilege enforcement, respectively.

Figure 3 expands on this analysis by applying a composite risk score (0-10 scale) in six enterprise risk domains. The biggest percentage changes are seen in audit visibility loss (8.0 to 2.2) and compliance gap (7.8 to 2.6), where the impact of the layer 5 governance controls including automated audit logging and regulatory mapping are realized. The underlying values of Figure 3 are reported in Table 3.

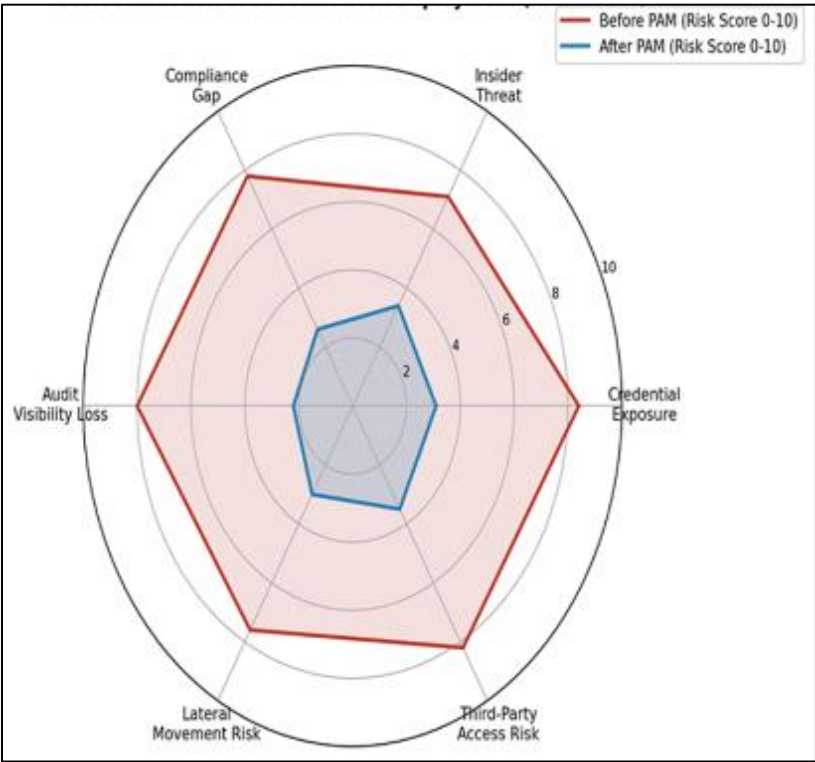


Figure 3: Composite enterprise risk score across six risk domains, before and after PAM framework deployment (illustrative).

Table 3: Illustrative mean risk scores across six risk domains before and after PAM implementation.

Risk Domain	Mean Risk Score - Before PAM (0-10)	Mean Risk Score - After PAM (0-10)
Credential Exposure	8.4	3.1
Insider Threat	7.1	3.4
Compliance Gap	7.8	2.6
Audit Visibility Loss	8.0	2.2
Lateral Movement Risk	7.6	3.0
Third-Party Access Risk	8.2	3.5

These results are illustrative, but directionally consistent with industry PAM maturity studies and qualitative research in regulated industries like healthcare that also show a correlation between multiple layers of PAM and measurable decreases in unauthorized access and insider-related incidents [5], [8]. The consistency in structure between the proposed framework and the patterns of improvement observed suggest that risk mitigation in privileged access management is strongest when technical controls (Layers 1-4) are combined with governance oversight (Layer 5), as opposed to being point solutions.

5.1 Compliance Mapping

One unique aspect of the proposed framework is that it expressly relates to more than one set of regulatory and standards requirements, which would enable a single PAM deployment to meet multiple requirements or obligations without having to implement duplicative, framework-specific controls. Table 2 correlates representative PAM capabilities with the NIST SP 800-53 Revision 5, ISO/IEC 27001:2022, PCI DSS v4.0, GDPR and HIPAA Security Rule clauses.

Table 2: Mapping of PAM control capabilities to major regulatory and standards frameworks.

Regulatory / Standards Framework	Relevant Clause / Control Family	PAM Control Alignment
NIST SP 800-53 Rev. 5	AC-6 Least Privilege; AC-2 Account Management	Role-based access, JIT provisioning, account lifecycle automation
ISO/IEC 27001:2022	Annex A.8 - Access Control	Privileged account inventory, periodic access review
PCI DSS v4.0	Requirement 7 & 8 - Access Restriction and Authentication	Credential vaulting, MFA on all administrative access
GDPR (Regulation (EU) 2016/679)	Article 32 - Security of Processing	Session logging, breach traceability, data-access minimization
HIPAA Security Rule	45 CFR 164.312(a) - Access Control	Unique user identification, emergency access, audit trails

This mapping illustrates how the core PAM capabilities—including least privilege, multi-factor authentication, and audit logging—are explicitly mentioned in each major framework evaluated here, and thus confirms that PAM should be viewed as an underlying and cross-cutting control and not as an optional security feature [10]-[14].

Challenges and Limitations

- Legacy system integration – many legacy applications hardcode credentials and will not vault without application level remediation.
- Organizational resistance: administrators who are used to the current standing access approach may view just-in-time provisioning as an operational burden, thus making it necessary to invest in change management [5].
- Third-party/Managed service provider access: managed service providers or contractors may need privileged access to the organization's resources but not be part of its core identity directory, making governance difficult.

In multi-cloud deployments, privileged identities are ephemeral, machine-based, and numerous, making them hard to manage with traditional PAM tooling. [4]

One drawback of the comparative metrics used in Section 5 is that they are illustrative and future research should be performed to validate the framework with longitudinal, organization specific telemetry rather than the representative estimates provided. Also, the five-layered framework is based on a minimum level of identity governance maturity (Layer 1), which not every organization has, and thus indicates a need for phased implementation roadmaps for organizations starting from a low level of maturity.

6 CONCLUSION AND FUTURE WORK

This paper has outlined a five-layer Privileged Access Management framework that combines identity foundation, credential and session management, access enforcement, monitoring and analytics, and governance and compliance into one coherent framework. Comparative illustrative analysis indicates that this layering can significantly diminish credential-based attack surfaces and enhance composite risk posture across multiple risk categories and meet requirements across NIST, ISO/IEC 27001, PCI DSS, GDPR and HIPAA. In the future, it is important to extend the PAM governance models to machine and non-human identities, as they will account for an increasingly larger portion of privileged access in modern enterprises, and provide empirical validation of the proposed framework using longitudinal organizational data, as well as deeper integration of artificial intelligence for continuous risk scoring.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Disclosure of conflict of interest

The authors declare no conflicts of interest regarding this manuscript.

REFERENCES

- [1] Haber, M. J. (2020). Privileged attack vectors: Building effective cyber-defense strategies to protect organizations (2nd ed.). Apress.
- [2] Liu, A., Du, X., & Wang, N. (2020). Access control role evolution mechanism for open computing environment. *Electronics*, 9(3), 517. <https://doi.org/10.3390/electronics9030517>
- [3] Bhargude, S. (2023). Advancing enterprise security: A framework for AI-powered privileged access posture management. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 9(6).
- [4] Moor Insights & Strategy. (2023). Modern privileged access management [Research paper]. Moor Insights & Strategy.
- [5] Rout, S. (2023). Privileged user access audits: Techniques for identifying and mitigating insider threats. *International Journal for Multidisciplinary Research*, 6(2).
- [6] SSH Communications Security. (2023). Challenges in cross-platform PAM implementation. SSH Academy.
- [7] Gartner. (2022). Magic quadrant for privileged access management. Gartner, Inc.
- [8] BeyondTrust. (2022). Seven steps to complete privileged access management [White paper]. BeyondTrust Corporation.
- [9] Verizon. (2023). 2023 Data breach investigations report. Verizon Business.
- [10] National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53, Rev. 5). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-53r5>
- [11] International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC 27001:2022).
- [12] PCI Security Standards Council. (2022). Payment Card Industry Data Security Standard (PCI DSS), Version 4.0.
- [13] European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union.
- [14] U.S. Department of Health and Human Services. (2013). HIPAA Security Rule, 45 C.F.R. §§ 164.302-318.
- [15] National Institute of Standards and Technology. (2020). Zero trust architecture (NIST Special Publication 800-207). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-207>
- [16] Cybersecurity and Infrastructure Security Agency. (2023). Zero trust maturity model, Version 2.0. U.S. Department of Homeland Security.