TECH HIVE
ADVISORY

Access Is Authority:

Why Privileged Systems Still Escape Governance

Introduction

Privileged Access Management (PAM) is widely[1] recognised within cybersecurity standards and governance frameworks as a critical control for protecting digital systems. Yet, insider-related incidents, access misuse, and system-level failures continue to occur even in organisations with formal PAM policies and audits in place[2]. This persistence suggests that the core challenge is no longer one of awareness but of execution. This article argues that failures in privileged access governance stem from structural gaps between policy and practice, static oversight mechanisms in dynamic digital environments, and the misplacement of access ownership within technical functions rather than enterprise risk structures. Addressing these gaps requires rethinking PAM not as a checklist control, but as a continuously governed form of organisational authority.

[1] 'Privileged Access Management (PAM)' (BeyondTrust) <https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam\> accessed 13 February 2026.

[2] 'The Impact of Privileged Access Management Frameworks on Reducing Insider Threats in Regulated Industries' (Prianka Syed, January 2026) https://www.researchgate.net/publication/399865454_The_Impact_of_Privileged_Access_Management_Frameworks_on_Reducing_Insider_Threats_in_Regulated_Industries accessed 13 Feburary 2026

What is Privileged Access Management?

In simple terms, Privileged Access Management is about controlling who has the highest level of access to an organisation's digital systems[3]. Some roles require more power than others, for example, the ability to change system settings, access sensitive data, create or delete user accounts, or disable security controls. PAM exists to make sure this kind of access is given only when necessary, limited to what is needed, and properly monitored. Without it, a small number of people can quietly hold more power over systems than the organisation realises.

The problem is that PAM is often treated as a technical setup rather than a governance issue. [4]Organisations may have tools in place, but not clear rules about who owns access decisions, how long access should last, or who reviews what privileged users actually do. When that happens, digital authority grows outside formal oversight. PAM, at its core, is therefore not just about security, it is about ensuring that power inside digital systems is exercised responsibly, transparently, and in line with organisational governance.

Why Privileged Access Continues to Escape Governance

Privileged access escapes governance because the way digital authority is exercised does not align with how organisational governance is designed to function.[5] Governance frameworks rely on visibility, clear ownership, and stable decision points. Privileged systems, by contrast, concentrate power within technical environments that operate continuously, change rapidly, and sit largely outside formal oversight structures. The result is not a lack of control, but a lack of governability.

Although standards such as ISO/IEC 27001, NIST SP 800-53, and COBIT 2019 require controls over privileged access, they primarily address whether controls exist, not how authority behaves once access is granted[6].

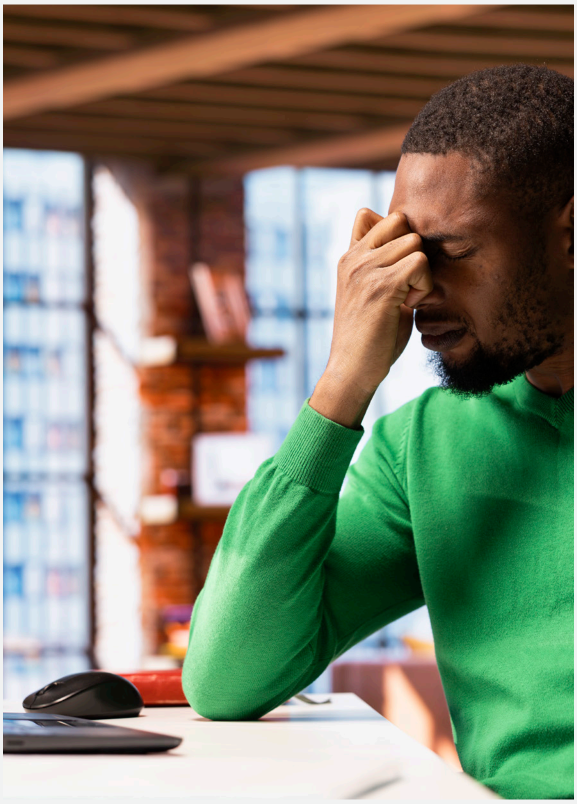
[3] BeyondTrust, 'Privileged Access Management (PAM)'
[4] 'Privileged access management' (ScienceDirect, Elsevier) https://www.sciencedirect.com/science/article/abs/pii/S1353485819301096 accessed 13 February 2026.
[5] Alfredo Santos, 'Privileged Access Governance: What It Is and Why It Matters' (IAM Tech Day, 18 December 2024) https://iamtechday.org/en/articles/privileged-access-governance-what-it-is-and-why-it-is-important/ accessed 13 February 2026.
[6] 'Integrating COBIT 2019 and ISO/IEC 27001 for Strengthening IT Governance and Information Security' (Proceedings of The International Conference on Computer Science, Engineering, Social Science, and Multi-Disciplinary Studies, Vol 1, 2025) https://www.researchgate.net/publication/398552151_Integrating_COBIT_2019_and_ISOIEC_27001_for_Strengthening_IT_Governance_and_Information_Security accessed 13 February 2026.

In practice, privileged actions are executed as routine system operations. Configuration changes, permission escalations, and account creations occur within authorised boundaries and are therefore recorded as technical activity rather than governance events. This allows significant authority to be exercised without triggering escalation, review, or challenge at the enterprise level.

The problem is compounded by the mismatch between static governance processes and dynamic digital environments[7]. Access reviews, audits, and compliance assessments are periodic by design, while digital systems evolve continuously. Cloud deployments, DevOps workflows, emergency fixes, and third-party integrations expand privileged access incrementally and often permanently. By the time governance mechanisms intervene, access has already drifted beyond its original justification, creating uncertainty over who holds effective control over critical systems.

Ownership further weakens governance. Privileged access is typically managed within IT or security functions whose primary responsibility is operational continuity. Decisions about access[8] are therefore made to restore services, meet delivery timelines, or resolve incidents, not to preserve governance integrity. Exceptions accumulate, temporary privileges persist, and access becomes normalised through use rather than reviewed through authority. Organisations may remain formally compliant, yet the distribution of digital power no longer reflects governance intent.

This is the core governance failure: privileged access is treated as a technical configuration when it functions as institutional authority. Until access decisions are governed with the same clarity, accountability, and oversight applied to financial or legal authority, privileged systems will continue to operate beyond effective governance control.



[7] 'Understanding Access Governance: Beyond RBAC – How Fine-Grained PBAC Controls Drive Business Success in a Digital Platform' (SafePaaS, 2024) https://www.safepaas.com/resources/Understanding-Access-Governance-Beyond-RBAC.pdf accessed 13 February 2026.

[8] 'Top 5 Poor Privileged Account Management Practices' (Syteca) https://www.syteca.com/en/blog/top-5-poor-privileged-account-management-practices accessed 13 February 2026.

Insider Risk as a Symptom of Governance Failure

Insider-related incidents are often framed as security failures or cultural problems. In reality, they are more accurately understood as symptoms of governance breakdown[9]. When individuals retain excessive, persistent, or poorly supervised access, the failure has already occurred at a structural level, long before any misuse becomes visible.

The persistence of insider risk, despite widespread adoption of Privileged Access Management tools, demonstrates the limits of technical controls in the absence of strong governance. Access restrictions may exist, but without continuous review, independent oversight, and clearly assigned accountability[10], they function as symbolic safeguards rather than effective constraints. In such environments, compliance is achieved, but authority remains weakly governed.

This dynamic is evident in well-documented cases of access-related failure. The Snowden disclosures revealed how a contractor was able to exploit[11] broad system-level privileges across multiple intelligence systems, not through technical intrusion, but through access that exceeded functional necessity and lacked effective oversight. Similarly, post-incident analysis of the Capital One breach highlighted how overly permissive cloud access roles and weak governance[12] over credential ownership enabled large-scale data exposure without triggering timely escalation. In both cases, actions appeared operationally legitimate within systems, even as they represented failures of access governance.

These risks intensify in high-growth and digitally complex environments, where systems scale faster than governance capacity. As technical roles expand and access becomes more distributed, privileged authority fragments across platforms, teams, and vendors. Without deliberate governance intervention, insider risk emerges not as an exception but as a predictable outcome of organisational complexity.

[9] 'Didier Cossin and Abraham Hongze Lu, 'Board Oversight of Cyber Risks and Cybersecurity' (IMD Research-Knowledge) https://www.imd.org/research-knowledge/corporate-governance/articles/board-oversight-cyber-risks-cybersecurity/ accessed 13 February 2026.

[10] Ibid.

[11] Luke Barr, 'How Snowden Did It' (NBCNews) https://www.nbcnews.com/news/world/how-snowden-did-it-flna8c11003160 accessed 13February2026.

[12] 'Real-World Breach Snapshot: Capital One — The Real Cost of Misconfigured Cloud Identities: How Excessive Privilege Becomes a Breach Path' (Clutch Events) https://www.clutchevents.co/resources/the-real-cost-of-misconfigured-cloud-identities-how-excessive-privilege-becomes-a-breach-path#:%7E:text=were%20in%20place.-,Real-World%20Breach%20Snapshot:%20Capital%20One,environments%2C%20and%20fixing%20configuration%20drift. accessed 13February2026.

Recommendations

Organisations should institutionalise[13] privileged access oversight by placing it under formal enterprise risk supervision rather than leaving it solely within IT or security functions. Boards should require the establishment of cross-functional access governance forums that include risk[14] management, compliance, internal audit, legal, and security leadership to jointly review high-risk privilege decisions and exception approvals. Access authorisations should be tied to documented business justification, defined expiry timelines, and automated escalation triggers where privileges exceed risk thresholds. Independent assurance functions should also be mandated to conduct targeted reviews of administrative accounts, emergency access usage, and dormant privileged credentials to identify governance drift. Contemporary cyber governance guidance emphasises that cybersecurity risks must be embedded into enterprise risk frameworks and subjected to independent oversight to ensure that operational priorities do not override governance accountability[15]. Similarly, privileged access governance best practice highlights the need for structured approval, auditability, and independent validation of privilege assignments to prevent uncontrolled accumulation of administrative authority.

Operational governance must also be strengthened by reducing permanent privileged access and replacing it with controlled[16], time-bound access models.

[13] 'Cyber Security Governance Principles' (Australian Institute of Company Directors(AICD), 2024) https://www.aicd.com.au/content/dam/aicd/pdf/tools-resources/director-tools/board/cyber-security-governance-principles-web3.pdf accessed 13 February 2026.

[14] Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (National Institute of Standards and Technology(NIST) Special Publication800-37Revision2, December2018) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf accessed 13February2026.

[15] AICD, Cyber Security Governance Principles.

[16] '10 Steps to Successful Privileged Access Management' (Gotyto) https://gotyto.com/thought-leadership/10-steps-to-successful-privileged-access-management/ accessed 13 February 2026.

Organisations should implement just-in-time privilege elevation, enforce strong authentication controls, and maintain full activity monitoring for sensitive administrative actions. Access governance checkpoints should be embedded into employee and vendor lifecycle processes so that role changes, project transitions, system integrations, and contract terminations automatically trigger privilege reassessment. Executive leadership must also receive structured reporting that translates access metrics into enterprise risk exposure indicators, enabling leadership to interrogate[17] privilege expansion decisions and monitor systemic access trends. Governance frameworks consistently stress that effective cyber oversight depends on leadership literacy and continuous monitoring mechanisms that allow organisations to detect privilege creep before it becomes a systemic risk. By integrating automated privilege control, lifecycle-driven review processes, independent assurance, and executive-level visibility, organisations can ensure that privileged access is governed as a persistent organisational authority rather than a background technical function.

Conclusion

Privileged access continues to escape effective governance because it sits at the intersection of speed, trust, and technical complexity, where organisational controls are weakest. Access decisions are routinely made to keep systems running, resolve incidents, or meet delivery timelines, and are rarely revisited once the immediate operational need has passed. Over time, these decisions accumulate into durable concentrations of authority that are invisible to traditional oversight mechanisms. Governance frameworks assume that power is exercised through formal processes and discrete approvals; privileged access, by contrast, is exercised continuously and often silently within systems. Until organisations design governance models that recognise access itself as a persistent form of authority, one that must be owned, reviewed, and constrained as conditions change, privileged systems will remain structurally capable of undermining the very controls meant to protect them.

[17] Ibid