
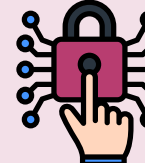










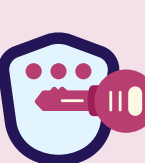



Introduction





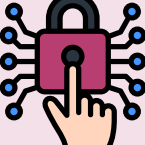

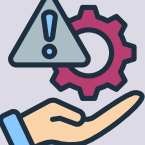
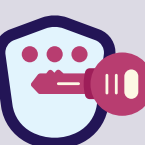






The National Institute of Standards and Technology (NIST) provides a comprehensive cybersecurity framework to help organizations manage and reduce risks. Privileged Access Management (PAM) plays a key role in ensuring compliance with NIST controls by securing privileged accounts, enforcing least privilege, and monitoring privileged activities. This document maps NIST controls to PAM capabilities, helping organizations enhance security and compliance.

NIST Control (SP 800-53 Rev. 5)

 <p>Enforce least privilege and manage user accounts.</p>	AC-2 Account Management	 <p>Role-based access control (RBAC), Just-in-Time (JIT) access, and automated access provisioning.</p>
 <p>Prevent conflicts of interest by segregating duties.</p>	AC-5 Separation of Duties	 <p>Enforced role separation and least privilege enforcement.</p>
 <p>Restrict system access to authorized users.</p>	AC-6 Least Privilege	 <p>Privileged access restrictions, session monitoring, and credential vaulting.</p>
 <p>Secure remote access mechanisms.</p>	AC-17 Remote Access	 <p>Agentless remote access, multi-factor authentication (MFA), and session recording.</p>
 <p>Ensure secure mobile device access.</p>	AC-19 Access Control for Mobile Devices	 <p>Conditional access policies and endpoint security controls.</p>
 <p>Implement strong authentication mechanisms.</p>	IA-2 Identification and Authentication	 <p>Multi-factor authentication (MFA) and passwordless authentication.</p>
 <p>Manage authentication credentials securely.</p>	IA-5 Authenticator Management	 <p>Credential vaulting, automated password rotation, and just-in-time access.</p>



NIST Controls		VS	PAM Capabilities	
	Capture security-related access events.	<b>AU-2 Audit Events</b>		Privileged session monitoring, keystroke logging, and real-time alerting.
	Generate logs for security monitoring.	<b>AU-12 Audit Generation</b>		Centralized logging and integration with SIEM solutions.
	Control access to system changes.	<b>CM-5 Access Restrictions for Change</b>		Change management enforcement and privileged approval workflows.
	Secure management of cryptographic keys.	<b>SC-12 Cryptographic Key Establishment and Management</b>		Secure vaulting and lifecycle management for privileged credentials.
	Ensure sensitive data is securely stored.	<b>SC-28 Protection of Information at Rest</b>		Encrypted credential storage and data masking.
	Monitor system behaviors and protect sensitive operations.	<b>SC-42 Sensor Capability and Data Protection</b>		Behavioral analytics, anomaly detection, and session auditing.

## Conclusion

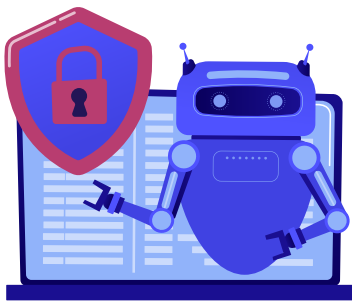


By aligning PAM solutions with NIST cybersecurity controls, organizations can enhance their security posture, reduce risk exposure, and achieve compliance. PAM ensures robust access control, secure authentication, and continuous monitoring of privileged activities.

## Next Steps:



Conduct a PAM maturity assessment aligned with NIST controls.



Implement automated privileged access management.



Establish continuous monitoring and auditing practices.

