

Introduction



ISO 27001 is a globally recognized standard for information security management, providing a framework to protect sensitive data. Privileged Access Management (PAM) plays a crucial role in addressing ISO 27001 controls related to access security, authentication, and privileged account management. This document maps key ISO 27001 controls to PAM capabilities, ensuring organizations can effectively implement and maintain compliance.

ISO 27001 Controls



Enforce least privilege and restrict access based on business requirements.

A.5.15  
Access Control



Role-based access control (RBAC), Just-in-Time (JIT) access provisioning, and enforcement of least privilege.



Ensure the secure management of identities, authentication, and authorization.

A.5.16  
Identity Management



Centralized privileged identity management (PIM) with secure authentication methods (MFA, password vaulting).



Grant, modify, or revoke access rights in a controlled manner.

A.5.18  
Access Rights



Automated access request workflows and approval mechanisms.



Restrict and control the use of privileged utilities and programs.

A.8.2 Privileged  
Utility Programs



Application control and session monitoring for privileged activities.

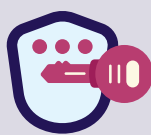


Implement strong authentication mechanisms to protect access.

A.8.3  
Secure Authentication



Multi-factor authentication (MFA) and passwordless authentication for privileged accounts.



Control and monitor access to sensitive code and configurations.

A.8.4 Access  
to Source Code



Privileged session management (PSM) with auditing and session recording.



Ensure secure log-on mechanisms are in place.

A.8.5 Secure  
Log-on Procedures



Secure remote access with agentless authentication and session recording.







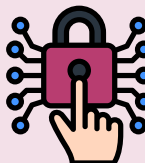



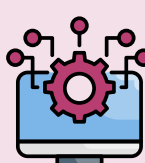



Restrict and manage privileged accounts, ensuring accountability.

A.8.8 Privileged  
Access Management



Privileged account discovery, lifecycle management, and credential vaulting.



ISO 27001 Controls	VS	PAM Capabilities
 Implement access monitoring and logging mechanisms.	A.8.10 Monitoring System Access	 Real-time privileged session monitoring, keystroke logging, and behavioral analytics.
 Secure storage and management of credentials.	A.8.12 Use of Secret Authentication Information	 Encrypted password vaults and automated credential rotation.
 Implement secure authentication techniques.	A.8.15 Secure Authentication Process	 Adaptive authentication and risk-based access controls.
 Maintain logs of security events for accountability.	A.12.1 Logging and Monitoring	 Centralized logging and integration with SIEM solutions.
 Ensure log data integrity and security.	A.12.2 Protection of Log Information	 Tamper-proof logging and privileged user behavior analytics.
 Restrict unauthorized access to critical system files.	A.12.6 Security of System Files	 File integrity monitoring and privileged session management.

## Conclusion

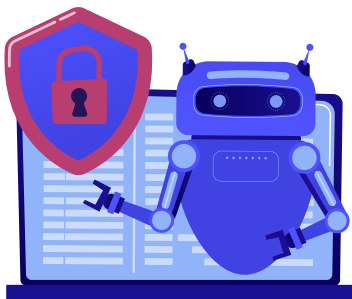


Implementing PAM solutions aligned with ISO 27001 controls helps organizations enhance their security posture, reduce attack surfaces, and ensure compliance. By integrating PAM capabilities, organizations can effectively manage privileged access, enforce least privilege, and maintain audit readiness.

## Next Steps:



Conduct a PAM maturity assessment aligned with ISO 27001.



Implement automated access control mechanisms.



Establish continuous monitoring and audit practices.

