Using PAM for Compliance

Introduction

Access management is critical to compliance with most security regulations, standards and frameworks. The goal of these standards is to ensure that unauthorized parties can't access sensitive data or systems and can't perform unauthorized modifications.

While access management is critical to compliance and security, privileged access management (PAM) is especially important. Privileged accounts have elevated access and rights within an organization's IT environments, and this access is critical to achieving a cybercriminal's objectives. PAM solutions help to manage and audit accounts with elevated permissions by restricting access based on least privilege, ensuring secure storage of login credentials and generating unalterable audit logs that track any actions these accounts perform.

Many cyberattacks involve compromised privileged accounts, and many standards, regulations and laws include explicit or implicit requirements to manage this access. Among these are:

- ISO 27001:2022
- UK Telecommunications Security Act
- PCI DSS v4.0
- Network Information Security Directive 2 (NIS2)_
- Health Insurance Portability and Accessibility Act (HIPAA)
- Sarbanes-Oxley Act (SOX)

Abstract

privileged access management (PAM) deals with the management and monitoring of accounts with elevated access and permissions within an organization's environment. The capabilities that PAM solutions provide are essential for compliance with many major regulations, such as PCI DSS and HIPAA, and security standards, such as ISO 27001:2022. Understanding regulatory requirements regarding privileged accounts is essential to understanding the role of PAM within a corporate cybersecurity and regulatory compliance strategy.

- National Institute of Standards and Technology (NIST) publications
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)
- SWIFT Customer Security Controls Framework (CSCF)
- Federal Information Processing Standards (FIPS)

Importance of PAM in general compliance

All the standards above require organizations to implement access controls – including PAM. However, PAM is also valuable for general regulatory compliance and corporate cybersecurity.

Some key benefits that it provides include:

- **Risk reduction:** PAM provides insight into and control over the use of elevated privileges within an organization's environment. This allows an organization to detect or prevent attacks attempting to abuse these privileges.
- **Accountability and monitoring:** Logging and monitoring is a central part of PAM. Detailed audit logs with integrity protection in place are essential for tracking the use of privileged accounts and holding users accountable for potential misuse or abuse of the rights assigned to them.
- **Incident response and management:** Compromised privileged accounts feature in many data breaches and other security incidents. PAM is a necessary tool for incident responders to understand the scope of an incident and to lock down access to compromised privileged accounts.

PAM for ISO 27001:2022 compliance

ISO 27001:2022 is an international standard that describes best practices for implementing information security management systems (ISMS). ISO 27001:2022 lays out requirements for PAM in Annex A Control 8.2, which states that organizations must manage and restrict the use of privileged accounts.

This explicit requirement for managing privileged accounts makes PAM essential for compliance with the standard. Organizations seeking accreditation against this standard will need to implement processes for assigning elevated privileges to users, authenticating their identities, auditing their activities and revoking permissions when needed.

PAM for Telco Security Act compliance

The Telecommunications Security Act is an act of the UK Parliament designed to enhance the security of telecommunications networks within the UK. While the Act doesn't explicitly mandate the use of PAM, it requires telcos to reduce its risk of security compromises, which includes "any unauthorised access to, interference with or exploitation of the network or service or anything that enables such access, interference or exploitation."

PAM is essential for compliance with this act due to the common role that compromised privileged accounts play in most security incidents. If a telco is required to take actions to decrease its risk of security compromises, then access management in general, and PAM in particular, is an essential component of its security strategy. Therefore, telecommunications providers will need to implement PAM as part of their broader strategy to comply with the act's requirements, particularly in managing and securing privileged access to critical infrastructure.

PAM for PCI DSS v4.0 compliance

The Payment Card Industry Data Security Standard (PCI DSS) v4.0 is a standard developed by the financial sector to protect cardholder data and prevent financial fraud. PCI DSS has several requirements related to PAM and access management, including:

- **Restrict access to cardholder data by business need to know:** Mandates that organizations implement least privilege access and manage access via access control systems. Additionally, account permissions should be reviewed every six months at the minimum.
- **Identify and authenticate access to system components:** Requires strong user authentication with a unique user identifier before granting access. Authentication to a system within scope of PCI-DSS must be performed via multi-factor authentication (MFA).
- **Track and monitor network access:** Specifies that all activities on the system must be recorded in audit logs, which will be reviewed at least daily.

PAM is indispensable for meeting the access management requirements of PCI DSS. Organizations need to be able to enforce the principle of least privilege, perform strong authentication and continually monitor user activity.

PAM is especially important for protecting cardholder data due to the significant risks associated with compromises of this data. Cardholder data can be used for financial theft, identity theft and other fraudulent activities. PAM helps to lock down access to the privileges required to carry out data breaches within an organization's environment.

PAM for NIS2 Compliance

The Network Information Security Directive 2 (NIS2) is a new legislation from the EU, which applies to member states as of October 2024. The goal of NIS2 is to mitigate and manage the often-complex cyber threats targeting European critical infrastructures. To prevent cyberattacks, the NIS2 Directive outlines a series of security measures that are mandated for essential and important entities within member states. Implementing PAM solutions helps organizations comply with these requirements, particularly those related to access management and privilege control.

Article 21 of NIS2 mandates that these essential and important entities take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the entities' security of network and information, and to prevent or minimize the impact of incidents on recipients of their services and on other services.

24

Article 23 mandates strict reporting requirements, including that significant incidents must be reported within 24 hours

Article 23 mandates strict reporting requirements, including that significant incidents must be reported within 24 hours, full notification to be issued within three days of being made aware of the incident and a final report issued within a month of the submission of the incident notification.

PAM is an essential component of any cybersecurity strategy aligned to meeting NIS2 regulatory requirements, as it applies controls such as session monitoring and recording, credential vaulting, Just-in-Time (JIT) Privileged Access, real time monitoring, automated response and remediation in addition to forensic audit trail capabilities. These controls directly assist in meeting Articles 21 and 23 of NIS2, which is required in order to avoid any potential fine from non-compliance.

PAM for HIPAA compliance

The Health Insurance Portability and Accessibility Act (HIPAA) is a U.S. regulation designed to protect patient privacy and ensure the security of protected health information (PHI). This regulation applies to healthcare providers or "covered entities (CEs)" and their business associates (BAs).

In 45 CFR § 164.312 (a) (1), HIPAA defines requirements for access control, which mandate that access to PHI should be restricted to authorized parties. Additionally, HIPAA requires CEs and BAs to audit login attempts and perform daily reviews of audit logs.

PAM solutions provide the access management and monitoring capabilities mandated by HIPAA. Organizations can restrict access to PHI using least-privilege access controls and audit that access to support incident response activities and regulatory reporting.

PAM for SOX compliance

The Sarbanes-Oxley Act (SOX) is a U.S. regulation designed to ensure the correctness of financial reporting by public companies. The regulation mandates that the company's CEO and CFO must sign off on the effectiveness of its internal controls, which should ensure the company's ability to "record, process, summarize and report financial data."

Access controls are essential for SOX compliance because they help to deter unauthorized access to and modification of financial data. Strict access controls minimize access to critical financial information, and audit logs can be used to identify and address any attempts to modify data to support or conceal fraudulent activity.

PAM contributes to financial accountability and transparency by enabling the CEO and CFO to attest to the accuracy of their reports. Without PAM, the potential exists that data may have been tampered with by privileged accounts in an attempt to conceal fraud or theft. With strict access controls and unalterable access logs, an organization can both prevent these potential threats and prove that no such fraudulent activities occurred.

PAM for NIST compliance

The National Institute of Standards and Technology (NIST) is a U.S. government agency tasked with developing standards and best practices on various subjects. Some notable cybersecurity resources developed by the agency include its Cybersecurity Framework (CSF), Risk Management Framework (RMF), and NIST SP 800-53.

NIST SP 800-53 is a widely-used standard titled, "Security and Privacy Controls for Information Systems and Organizations". Some relevant controls within the standard include:

- **AC-5 Separation of duties:** Divides critical or sensitive business flows across multiple parties to reduce the risk of fraud and other potential threats.
- **AC-6 Least privilege:** Minimizes the privileges assigned to a user to include only those required for their duties. This includes restricting access to privileged functionality and requiring privileged users to use non-privileged accounts for actions that don't require those privileges.
- **AU-6 Review and audit system audit records:** Requires regular reviews of audit logs, including performing full-text analysis of privileged access logs on a system other than the one where the user has privileged access.
- **IA-2 Identification and authentication:** Requires the use of MFA for authentication to privileged accounts.

NIST SP 800-53 details cybersecurity best practices, and compliance is mandatory for U.S. federal agencies. PAM is required for compliance with requirements AC-6, AU-6, and IA-2 at a minimum, since the agency must be able to ensure that privileged accounts are used only when necessary and are secured with strong access controls. It is also helpful in streamlining compliance with other access control requirements, such as auditing and monitoring user activities on federal systems.

PAM for NERC CIP compliance

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) program is intended to ensure the reliability of the power sector, including protection against threats such as cyberattacks. The CIP's requirements include:

- **CIP-004-6 R4 Access management program:** Mandates that Responsible Entities (REs) implement an access management program that includes least privilege access and access reviews at least once every 15 calendar months.
- **CIP-007-6 R5 System access control:** Defines requirements for a system access control policy, including user authentication, password policies and account lockouts after unsuccessful login attempts.

The energy sector is critical infrastructure, making it a high-risk target for cyber threat actors. PAM is especially critical in this sector since abuse of elevated privileges and access could permit an attacker to disrupt electricity generation and distribution.

The SWIFT network is used to **transfer** money between banks, making **access management** a **critical** component of a financial institution's **cybersecurity** strategy.

PAM for SWIFT compliance

The SWIFT Customer Security Controls Framework (CSCF) describes required and optional security controls for users of the SWIFT financial transfer network. The CSCF has a few requirements related to access management, including:

- 4. Prevent compromise of credentials: Lays out requirements for password policies and the use of MFA to secure accounts.
- 5. Manage identities and separate privileges: Applies the principles of least privilege, need-to-know and separation of duties for logical access management.
- 6. Detect anomalous activity to systems or transaction records: Requires that processes and policies be in place to identify suspicious login activities and report them to the security team.

The SWIFT network is used to transfer money between banks, making access management a critical component of a financial institution's cybersecurity strategy. Without proper access controls, an attacker will be able to generate fraudulent messages, resulting in unauthorized transfers of funds into attacker-controlled accounts.

In the financial sector, most high-risk activities are performed by privileged accounts. PAM monitors and controls the use of these accounts, reducing their risk of compromise and improving the probability that fraudulent activities will be detected and remediated before significant damage is done.

PAM for FIPS compliance

The Federal Information Processing Standards (FIPS) are developed by NIST and define requirements for U.S. government computing systems. FIPS 200, titled "Minimum Security Requirements for Federal Information and Information Systems," includes requirements for access control, stating that "Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise."

FIPS compliance requires implementation of the security controls outlined in NIST 800-53. PAM is an essential component of a NIST 800-53 compliance strategy for federal agencies due to the need to manage and monitor use of privileged accounts.

Conclusion

Access management is central to the mission of most cybersecurity regulations and standards since they are designed to protect sensitive data and high-risk functionality. PAM is especially important due to the greater range of malicious actions that an attacker could perform with access to a privileged account.

Implementing PAM is necessary for a corporate compliance strategy but also benefits the organization's security in general. Compromised privileged accounts are fundamental in cyberattacks, and controlling access to these accounts will reduce the risk of an attack or an attacker's dwell time within an organization's network. This reduces the potential financial, reputational and operational damage that an organization will incur as a result of an attack.

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Access Management (AM), Privileged Access Management (PAM) and Active Directory Management (AD Mgmt) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 250 million identities for more than 5,000 organizations worldwide. For more information, visit www.oneidentity.com.