FUDO | ENTERPRISE

FUDO

THE KEY TO COMPLIANCE:

Using PAM to Meet ISO/IEC 27001 Standards

Start a 30-Day Evaluation →

www.fudosecurity.com

1. Introduction

In the context of PAM, organizations must find a balance between enabling efficient access to systems and data for authorized users and preventing unauthorized access and excessive permissions. Decisions made in this area must be thoroughly analyzed concerning the organization's specifics and its goals.

Guidelines for achieving this balance can be found in ISO/IEC 27001, an international standard that outlines the requirements for an Information Security Management System (ISMS). Its significance for organizations extends beyond mere regulatory compliance; it serves as a testament to maturity in information security management and digital trust. Implementing ISO/IEC 27001 not only strengthens data protection but also positively impacts the company's reputation by increasing trust among customers and business partners while contributing to the identification and effective management of risks associated with information processing. This standard offers a solid foundation on which organizations can build and develop their security strategies.

In the context of PAM, ISO/IEC 27001 provides clearly defined action frameworks that help organizations systematically analyze, implement, and monitor controls related to access management and identity, creating a robust basis for protecting their most valuable assets—data.

1.1. Purpose of ISO/IEC 27001

The ISO/IEC 27001 standard provides organizations with a set of requirements that facilitate the establishment, implementation, maintenance, and continuous improvement of an Information Security Management System

(ISMS). This standard emphasizes the protection of confidentiality, integrity, and availability of information through the application of rigorous risk management procedures and the implementation of appropriate security measures. The key objectives that ISO/IEC 27001 aims to achieve include:

ENSURING DATA CONFIDENTIALITY:

Protecting information from unauthorized access and disclosure.

MAINTAINING INFORMATION INTEGRITY:

Safeguarding data against unauthorized changes and ensuring that information is accurate and complete.

GUARANTEEING AVAILABILITY:

Ensuring that authorized users have access to information and related resources when needed to carry out their assigned tasks.

ISO/IEC 27001 also helps organizations meet legal and regulatory requirements related to information security, enhance trust among customers and other stakeholders by demonstrating commitment to information security, and minimize risks associated with data processing. Implementing and certifying according to ISO/IEC 27001 demonstrates that an organization adopts a professional approach to managing the security of its information, which can be a significant competitive advantage and build its reputation in the market.

2. Understanding ISO/IEC 27001

2.1. Structure of the Standard

The content of the standard can be divided into two main parts:

Requirements for the Information Security Management System (ISMS) (clauses 4-10), which cover the context of the organization, leadership, planning, support, operational actions, performance evaluation, and improvement.

Annex A, which includes recommended controls and control groups that organizations can implement to manage information security risks. Annex A is updated in response to evolving threats and new technologies, providing a framework for specific actions aimed at protecting information. performance.

2.2. Main Requirements of the Standard

ISO/IEC 27001 requires organizations to conduct regular risk assessments and implement appropriate controls based on the results of the risk management process. These controls may encompass organizational, physical, and technological aspects of information security.

BASED ON CLAUSES 4 TO 10 OF THE STANDARD, IT CAN BE SUMMARIZED THAT ISO/IEC 27001 REQUIRES ORGANIZATIONS TO:

Understand the needs and expectations of interested parties related to the ISMS and define its scope accordingly.

Ensure management involvement in ISMS processes by:

- Establishing information security policies,
- Ensuring that security objectives align with the organization's strategic direction,
- Assigning roles and responsibilities to designated individuals to ensure ISMS compliance with ISO/IEC 27001 and reporting on ISMS performance.

Identify and plan actions to manage information security risks and establish and control information security objectives. This includes risk assessment (identifying, analyzing, and evaluating risks) and risk management (selecting and implementing appropriate controls to reduce risk to an acceptable level). This clause requires organizations to plan these actions methodically and document the risk management process.

Ensure appropriate resources, competencies, awareness, and communication necessary for the effective establishment, implementation, maintenance, and continual improvement of the ISMS. This also includes documentation requirements. The standard emphasizes the importance of engaging all employees and providing them with the necessary support to adhere to the information security standards set by the organization.

Assess information security risks and implement appropriate controls to manage them.

Conduct systematic evaluations, monitoring, and audits to:

- Verify and maintain ISMS compliance with the standard's requirements, as well as the organization's objectives and needs,
- Verify the correctness of the implementation and maintenance of the ISMS.

Continually improve the ISMS by responding to non-conformities with the standard, striving to eliminate them, and documenting actions taken.

Achieving and maintaining ISO/IEC 27001 certification requires commitment from all levels and functions of the organization, as well as ongoing monitoring and review of the information security management system to ensure its effectiveness against new challenges in information security. ISO/IEC 27001 certification is globally recognized as proof that an organization employs a rigorous approach to managing its information security.

2.3. The Importance of Access Management in the Context of ISO/IEC 27001

Access management is a key aspect of the Information Security Management System (ISMS), as required by ISO/IEC 27001, because it controls who has access to information and systems and how that access is granted and monitored. Effective management aims to prevent unauthorized access to information, which is essential for protecting the confidentiality, integrity, and availability of data. This requires the implementation of policies and procedures such as:

- Minimizing access privileges to resources only to the extent necessary to perform specific tasks.
- Implementing role-based or identity-based access controls.
- Conducting regular reviews of granted access privileges.

Access management within the ISMS also helps organizations meet legal and regulatory compliance requirements, build trust with customers and business partners, and protect against internal and external security threats.

3. Introduction to PAM

3.1. Definition of PAM

PAM (Privileged Access Management) is a set of tools and practices used to manage and monitor access to privileged user accounts, such as system

administrators, users with access to sensitive data, or industrial control systems. PAM systems assist in the identification, authorization, and auditing of privileged user activities, minimizing the risks of data leaks, misuse, or external attacks.

REMOTE ACCESS SECURITY:

By limiting access to privileged accounts, PAM prevents potential attacks on critical resources.

PRIVILEGE MINIMIZATION:

The principle of least privilege restricts user access to only what is necessary, reducing the risk of misuse.

POLICY-BASED ACCESS MANAGEMENT:

It ensures that third-party engagements comply with relevant regulations (like GDPR or HIPAA), protecting the organization from legal and financial repercussions.

MULTI-FACTOR AUTHENTICATION (MFA):

Allows precise definition of who can access privileged resources and under what circumstances.

MONITORING AND AUDITING:

Adds an extra layer of security by requiring users to verify their identity using two or more verification methods.

THREAT ANALYSIS AND RESPONSE:

PAM decreases the attack surface by managing permissions according to the Zero Trust principle, granting access only to specific data and resources necessary for the task.

INDISPUTABLE EVIDENCE:

Data collected during remote sessions can serve as evidence in security

breach investigations. Timestamping the recorded session adds credibility to the material as legal proof.

PASSWORD MANAGEMENT:

PAM automates the management of strong, unique passwords, enhancing access security.

INTERNAL ABUSE PREVENTION:

By restricting privileges to only necessary resources, PAM helps reduce the risk of intentional or accidental harmful actions by employees.

INCREASED COMPLIANCE WITH REGULATIONS:

PAM helps meet legal and industry standards for access management and data security, such as the European NIS 2 Directive, GDPR, and international frameworks like NIST Cybersecurity Framework 2.0.

3.2. Why PAM Is Critical for Information Security

PAM (Privileged Access Management) refers to strategies and technologies used to control, monitor, and manage privileged access to an organization's most critical and sensitive resources and systems. Here are the key areas where PAM plays an essential role:

REDUCING THE ATTACK SURFACE

Privileged accounts are attractive targets for cybercriminals due to the extended permissions they offer. PAM significantly reduces the attack surface by limiting the number of individuals and systems with access to critical resources, making it more challenging for potential attackers to gain control over sensitive systems.

RISK MANAGEMENT AND COMPLIANCE

Implementing PAM enables organizations to manage risks associated with privileged access more effectively and helps maintain compliance with regulatory requirements and standards, such as ISO/IEC 27001. Organizations can respond promptly to external and internal audit requirements by demonstrating effective security controls.

LIMITING THE IMPACT OF DATA BREACHES

In the event of a security breach, having an implemented PAM solution can significantly limit the extent of the damage. By restricting privileged access to only those users who absolutely need it and rigorously monitoring this access, PAM allows organizations to quickly identify and respond to security incidents.

STRENGTHENING SECURITY POLICIES

PAM plays a crucial role in reinforcing an organization's security policies by enforcing principles of least privilege and segregation of duties. These practices ensure that users only have the permissions necessary to perform their jobs, minimizing potential harm from privilege misuse.

ENHANCING VISIBILITY AND CONTROL

PAM systems provide comprehensive visibility and control over privileged access across the organization. Real-time recording and monitoring of privileged sessions, along with advanced analytical tools, enable the quick detection of unauthorized or suspicious activities, significantly enhancing overall information security.

4. How Fudo Enterprise Supports ISO/IEC 27001 Compliance

Fudo Enterprise can help meet the control measures from Annex A of the ISO/IEC 27001 standard, either directly or indirectly, in the following areas:

1. ORGANIZATIONAL CONTROL MEASURES:

— Access Control
— Identity Management
— Authentication
— Access Permissions
— Evidence Collection
— Data Asset Protection

1. ORGANIZATIONAL CONTROL MEASURES:

— Remote Work

1. ORGANIZATIONAL CONTROL MEASURES:

— Privileged Access
— Restriction of Access to Information
— Secure Authentication
— Redundancy of Information Processing System Components
— Event Logging
— Activity Monitoring

The following table provides selected control measures along with a brief description of how Fudo Enterprise supports them.

A5. Organizational Controls

Annex	Control Type	Support Fudo Enterprise
A5.1	Policies for Information Security	Fudo Enterprise ensures that privileged access to sensitive information is controlled, monitored, and documented in alignment with the organization's information security policies.
A5.2	Information Security Roles & Responsibilities	Fudo Enterprise defines and controls user roles, ensuring that Auditors, Approvers, Administrators, and Users have specific, limited access, with all actions thoroughly logged and audited.
A5.3	Segregation of Duties	Fudo Enterprise enforces segregation of duties by separating conflicting roles and responsibilities, ensuring that no single user has unchecked access, and logging all actions to reduce the risk of errors or fraud.
A5.7	Threat Intelligence	Fudo Enterprise delivers tools that enable organizations to understand their threat environment and effectively identify, assess, and respond to emerging security threats.
A5.15	Access Control	Fudo Enterprise offers mechanisms for effectively monitoring and controlling remote access to systems and data. This enables the organization to establish access policies and track and record user activity to ensure information security.
A5.16	Identity Management	Fudo Enterprise indirectly supports user account management by automatically synchronizing user definitions with the Active Directory server or other LDAP-compatible systems.
A5.17	Authentication Information	Fudo Enterprise employs strong authentication mechanisms, including multi-factor authentication (MFA), providing additional layers of security for privileged access. Its password management tools eliminate the risk associated with weak or repetitive passwords while offering secure storage and regular updates. Administrators also have the option to configure Single Sign-On (SSO), which hides authentication credentials from users and ensures the use of strong passwords for accessing critical resources.
A5.18	Access Rights	Fudo provides tools for comprehensive management of access permissions to information and related resources. The platform enables effective creation, review, modification, and removal of access rights in accordance with organizational policies and access control principles defined for specific resources. With Fudo, organizations can establish and implement customized access policies that specify who, when, and how individuals can access particular resources.
A5.22	Monitoring, Review & Change Mngmnt of Supplier Services	Fudo Enterprise aids by enabling supplier segmentation, automated monitoring, review, and auditing of service delivery processes, including session sharing, approval workflows for suppliers, and ensuring proper documentation and change control management.

Annex	Control Type	Support Fudo Enterprise
A5.24	Information Security Incident Management Planning & Preparation	Fudo Enterprise supports compliance by enabling automated session monitoring, real-time alerts, logging, and auditing, while utilizing user roles and approval workflows to control access and manage security incidents.
A5.28	Collection of Evidence	With the implementation of Fudo Enterprise, administrators can automatically track and document all privileged activities within the IT infrastructure. The system also allows for detailed analysis of archived sessions to search for evidence of breaches, which is crucial in the event of cybersecurity incidents. Reporting features enable effective tracking of access paths and operations performed by users, allowing for the quick identification of threat sources and the implementation of appropriate corrective actions. Data collected during remote connections can serve as evidence in a security breach case. Timestamping recorded sessions makes the material a more credible piece of evidence.
A5.33	Protection of Records	This control measure requires the protection of assets from loss, destruction, or unauthorized access. Fudo Enterprise ensures that only authenticated users have remote access to resources.
A5.34	Privacy & Protection of PII	Fudo supports organizations in ensuring compliance with data protection regulations, such as GDPR, by controlling and monitoring user access to data.
A5.36	Compliance With Policies, Rules & Standards for Information Security	Fudo Enterprise supports business-specific compliance reporting, helps managers identify and address non-compliance issues, and tracks corrective actions. This facilitates timely resolution and documentation of progress for continuous improvement.
A5.37	Documented Operating Procedures	Fudo Enterprise supports compliance by ensuring detailed logs and session recordings for consistent activity tracking. The solution also facilitates monitoring and audit trails, provides clear escalation procedures, and ensures regular reviews and updates to procedures for optimal performance and security.

A6. People Controls

Annex	Control Type	Support Fudo Enterprise
A6.7	Remote Working	Fudo Enterprise ensures the security of task execution during remote work primarily by securing remote access to servers and data through advanced authentication methods. Sessions initiated using Fudo Enterprise can be monitored live and recorded, providing full control over user activities.

A8. Technological Controls

Annex	Control Type	Support Fudo Enterprise
A8.2	Privileged Access Rights	Fudo Enterprise supports organizations in controlling and limiting the assignment and use of privileged access rights. Fudo allows for the implementation of strict policies that restrict the granting of privileged access only to necessary resources and monitor their usage. This ensures effective management of access to key systems and data and helps minimize the risks associated with excessive privilege and potential threats to information security.
A8.3	Information Access Restriction	Fudo Enterprise is a comprehensive solution that enables effective management of remote access to an organization's resources. Administrators can monitor user activity and respond quickly in the event of a security breach. The platform provides full control over access, allowing administrators to precisely define who can access resources, when, and how. Additionally, administrators can set time restrictions for granted access, increasing security by controlling the duration of access to data.
A8.5	Secure Authentication	Fudo Enterprise also employs robust authentication mechanisms, including multi-factor authentication (MFA), providing additional layers of security for privileged access. The password management tools in Fudo Enterprise mitigate the risks associated with weak or repetitive passwords while offering secure storage and regular updates. Administrators also have the option to configure Single Sign-On (SSO) mechanisms, which hide authentication credentials from users and ensure the use of strong passwords for access to critical resources.
A8.14	Redundancy of Information Processing Facilities	Fudo Enterprise provides redundancy for session data and its own configuration. The Fudo Enterprise cluster ensures uninterrupted access to servers in the event of a node failure and also allows for the implementation of load-balancing scenarios for user queries.
A8.15	Logging	Fudo Enterprise features event logging functionality that records events occurring during connection establishment, throughout the session, and at its termination. Additionally, sessions established using Fudo Enterprise are recorded and can be reviewed at a later time.
A8.16	Monitoring Activities	By using Fudo Enterprise, organizations can monitor and document sessions to enhance transparency of activities on privileged accounts and maintain a searchable archive of user actions. This supports regulatory compliance and enables access analysis in the event of suspicious activity detection. With streamlined monitoring of privileged accounts, companies can effectively protect their most critical assets.

A8.21	Security of Network Services	Fudo Enterprise supports compliance by offering comprehensive logging and monitoring of network service access. It provides detailed records of access, including timestamps, user identities, and device data, while indirectly enhancing network security controls. For instance, by managing privileged access and reducing reliance on less secure remote access methods like VPN, TeamViewer, and VNC, Fudo Enterprise helps to harden the network perimeter and ensures that service providers meet their security and service level requirements effectively.
A8.34	Protection of Information Systems During Audit Testing	Fudo Enterprise supports compliance by providing comprehensive event logging and full session recording, which are crucial for maintaining detailed audit trails. This functionality ensures transparent access management, facilitates agreement on audit scope, and supports the review of access actions. Its robust logging helps document and monitor privileged access, aiding in regulatory adherence and safeguarding sensitive information during audits.

5. The Future of PAM and ISO/IEC 27001

5.1. The Evolution of ISO/IEC 27001 Standards and Future Changes

The evolution of ISO/IEC 27001 standards is an ongoing process, reflecting changes in technology, business practices, and information security threats. Since its first publication in 2005, the standard has undergone several updates, including a significant revision in 2013. Future changes will likely continue the trend of increasing flexibility, effectiveness, and coverage, taking into account emerging technologies such as cloud computing, artificial intelligence, and the Internet of Things (IoT). Adapting to the ever-expanding cyber landscape and evolving threats will be crucial to maintaining the standard as a reliable reference point for information security.

5.2. The Development of PAM Technology and Its Impact on Future Compliance Requirements

Privileged Access Management (PAM) technology is continuously evolving to meet the growing needs of organizations for information security. As cyber threats and the complexity of IT infrastructures advance, PAM becomes an essential tool in safeguarding critical systems and data.

The development of new PAM technologies, such as advanced behavior analysis features based on artificial intelligence, autonomous access management, and integration with security monitoring tools, may be a crucial factor influencing the evolution of future compliance requirements. Organizations will be required to incorporate these new capabilities into their information security strategies to effectively manage privileged access and meet increasing regulatory and normative expectations.

5.3. Relevant Documents and Legal Acts

DIRECTIVE 2008/114/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 8 DECEMBER 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve its protection (published in the Official Journal L 345, 23.12.2008).

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 14 DECEMBER 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive) (published in the Official Journal L 33, 27.12.2022).

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR) (published in the Official Journal L 119, 4.5.2016).