ManageEngine
PAM360

The compliance benefits of adopting PAM360

PAM solutions play a pivotal role in helping enterprises stay compliant and audit ready. Using the below checklist, you can identify all the features of PAM360 that will facilitate compliance and audit readiness.

A non-negotiable requisite

Compliance standards help enterprises validate and ensure their sensitive systems and data are safe from cyberthreats. Compliance with these standards strengthens an enterprise's cybersecurity and helps build trust with customers and partners. Non-compliance often results in business disruptions, governmental fines and penalties, (settlement costs, productivity losses, and more) that cost enterprises over $14 million on average. Compliance readiness is no longer just a good-to-have luxury, it's a vital requisite.

Meet compliance demands at your enterprise

Leading analyst firms highlight that compliance-readiness is one of the primary factors fueling rapid adoption of privileged access management solutions. By adopting a comprehensive solution like ManageEngine PAM360, your enterprise will receive a PAM solution that's compliant with major industry standards out of the box, helping you address the pressing needs of regulatory compliance and audit requirements.

Enterprise-ready solution, compliant out of the box

Just as with any other solution from ManageEngine, PAM360 is compliant with a wide array of privacy and compliance standards. These accreditations are industry gold-standards that assure you of our approach to privacy and security.

The top 7 ways PAM360 helps you meet compliance demands

PAM360's core features help businesses regulate access to sensitive information, maintain data integrity, and thereby comply with various regional and industry regulations. The following features are easy to setup and offer tangible compliance benefits.

Standards and Regulatory Requirements	Feature Required at least in part by the standards and regulatory requirements	Role of PAM360
GDPR (Article 32), ISO/IEC 27001: 2013 (9.4.1) [old], ISO/IEC 27001: 2022 (A 8.3) [new]	Enforce least privilege	Enterprises must adopt the principle of least privilege to ensure that end users have the lowest access privileges required to perform their tasks. PAM360's role-based access controls and just-in-time privilege elevation can help admins enforce least privilege access and minimize unauthorized access across every function within your organization.

HIPAA (164.312(a)(1)), ISO/IEC 27001: 2013 (A.9.2) [old], ISO/IEC 27001: 2022 (A 8.2) [new], GLBA (Section 501 b), and PCI-DSS (Requirement 7)	Fine-grained access provisioning	Access control is essential in streamlining access provisioning. PAM360's request-release workflow helps admins grant need-based access to authorized business users for valid tasks. This efficiently limits access to mission-critical systems and data.
PCI DSS (Requirement 8), and ISO/IEC 27001: 2013 (A.9.3)	Custom password policies and password rotation	Strict password policies enforce password hygiene across the organization. You can set up password policies that suit your organization's security policies, password reset schedules using PAM360.
HIPAA 164.308(a)(5)(ii)(C), SOX (Section 802 and Section 404), NIST SP 800-53 (AC-20(3)), and PCI-DSS Requirement 10.3	Remote session monitoring and termination	Session monitoring is vital in detecting suspicious activities in real time. With PAM360's extensive privileged session management capabilities, admins can stay on the lookout for anomalous activities as and when they occur, terminate sessions remotely, record every action performed on the endpoints, and more.

HIPAA (164.312(e)(1)), GDPR (Article 32 (1 a)), ISO/IEC 27001: 2013 (10.1.1), ISO/IEC 27001: 2022 (A 8.24) [new], and FedRAMP (AC-16, and AC-17)	Certificate lifecycle management	Proper management of SSL/TLS certificates in the business environment is vital to keep your business from outages and cyberthreats. PAM360 offers complete certificate lifecycle management capabilities to help users discover all their certificates, create, renew, and deploy new certificates, generate custom alerts for certificate expiry, and more. By doing so, enterprises can ensure that their critical systems are always encrypted and secure.
SOC 2 (CC6.2:03), ISO 27001:2013 (A.12.4.3), PCI-DSS (Requirement 10.2)	Real-time audits	PAM360's real-time audits continuously monitor and capture all sensitive activity performed by users. Enterprises can create a new account for auditors and add them to PAM360 as Password Auditors. Such users receive seamless access to all privileged access audits and reports.

Ready-made compliance reports

In addition to the above mentioned features, PAM360 offers ready-made reports that present an overview of all critical privileged management actions performed by users. As part of this offering, admins can generate dedicated reports for compliance standards like PCI-DSS, ISO-IEC 27001, NERC-CIP, and GDPR in a few clicks. You can find violations if any, and address them instantly.

Apart from the above listed features, PAM360 also offers end-to-end resource and account discovery, secrets management, self-service privilege elevation, application credential management, privileged user behavior analytics, and much more that help meet various compliance needs, and improve your organization's overall security posture.

Explore all features of PAM360

Compliance with other local regulations

PAM360's features help you adopt a compliance-first approach to numerous local compliance regulations. The following standards require enterprises to adopt various privileged access management features to attain compliance:

Standards and Regulatory Requirements	Subsections or requirements fulfilled	Role of privileged access management solutions
Cyber Essentials - United Kingdom	**User Access Controls** - One of Cyber Essentials' five requirements. It requires stringent access control policies to regulate access to "email, web and application servers; desktop computers; laptop computers; tablets; mobile phones with a focus on managing highly privileged accounts such as administrative accounts.	With the help of PAM360, enterprises can set up request-release workflows and role-based access controls to regulate access to mission-critical endpoint.
The Personal Data Protection Act (PDPA) - Singapore	**Section 24: Protection of personal data.** An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent — (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and	PAM360 can enhance the security of internal systems by safely managing and regulating access to such systems, thereby minimizing unauthorized access to personal data.

	(b) the loss of any storage medium or device on which personal data is stored.	
The General Data Protection Law (LGPD) - Brazil	**Portion of Article 46 states:** Processing agents shall adopt security, technical, and administrative measures to protect personal data from unauthorized accesses, and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing.	With advanced features such as role-based access control, policy-based access control, command control, and just-in-time elevation, PAM360 equips you with the right set of features to prevent unauthorized access of sensitive information.
Protection of Personal Information (APPI) - Japan	**Article 20:** A business operator handling personal information shall take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the personal data. **Article 22:** When a business operator handling personal information entrusts an individual or a business operator with the handling of personal data in whole or in part, it shall exercise necessary and appropriate supervision over the trustee to ensure the security control of the entrusted personal data.	By enforcing least privilege with role-based access control and just-in-time privilege elevation, and with privileged session auditing, monitoring, and management capabilities of PAM360, enterprises can prevent unauthorized access to personal data and audit every session launched.

Essential 8 - Australia	**Application Control, Restrict Admin Access (All three maturity levels)** - Part of the Essential 8 requires the following: Allow access to only required applications on systems and limit access to sensitive systems data.	With PAM360's command control, remote app access, and request-release workflows, enterprises can restrict access to administrative accounts and grant need-based, restricted, app-only access to critical devices. Additionally, enterprises can also mandate multi-factor authentication (MFA) when accessing PAM360 to secure their sensitive business accounts further.
Personal Information Protection and Electronic Documents Act (PIPEDA) - Canada	**Principle 4.7 - Safeguards** **(Principle 4.7.1):** The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.	PAM360's rigorous access control, command control, and remote app access features help protect personal data from unauthorized access by preventing privileged users from running unauthorized commands and by restricting their overall access.
Protection of Personal Information Act (POPIA) - South Africa	**Section 17** A responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of the	The security and integrity of personal data can be upheld by implementing role-based access control, request-release workflows, and just-in-time access provisioning features offered by PAM360.

	Promotion of Access to Information Act. **Section 19:** Security measures on integrity and confidentiality of personal information. The Section 19 requires responsible parties to ensure the integrity and confidentiality of personal information by implementing reasonable technical and organizational measures. Responsible parties must prevent loss, damage, or unauthorized destruction of personal information, as well as unlawful access or processing. This involves identifying risks, establishing safeguards, regularly verifying their effectiveness, and updating them as new risks emerge. Responsible parties should consider accepted security practices and procedures applicable to their industry or profession.	In addition, PAM360 can also monitor and record all activities performed by privileged users, along with real-time audits that document all the critical actions performed by users and admins.

The above listed compliance standards is not an exhaustive list. Using PAM360, you can stay compliant with various local and international regulations.

Get started with ManageEngine PAM360

To learn how PAM360 can help you in this journey, set up a free call with our experts.

Talk to our experts

Try PAM360 for free