The CISO's Guide to Regulatory Compliance

Quickly Meet Regulatory Compliance and Improve Security with PAM

WALLIX
TRACE, AUDIT & TRUST

The CISO's Guide to Regulatory Compliance

Quickly Meet Regulatory Compliance and Improve Security with PAM

ABSTRACT:

Firm but flexible control over privileged access sits at the root of many compliance measures. Effective management of privileged users enables fast, economical, and efficient compliance. Deficient privileged access management (PAM) can lead to the opposite: erroneous or even negligent non-compliance. PAM lowers the time it takes to meet regulatory compliance requirements by streamlining operations with ISO 27001, GDPR, and a host of comparable regulatory regimes.

WALLIX
TRACE, AUDIT & TRUST

INTRODUCTION

Despite the potentially overwhelming scope of compliance responsibilities, most regulatory schemes actually have similar core requirements. Slight differences emerge by sector and the protection levels required for various data assets. Differences aside, firm but flexible control over privileged access is a root factor in many regulations.

Compliance regimens like ISO 27001 and GDPR specifically mandate strong control, transparency, and audit logging of privileged (admin) users and their account sessions. Indirectly, other controls rely on Privileged Access Management (PAM) to ensure that only authorized users are performing essential tasks such as data encryption and network configuration. As a result, a well-run PAM solution streamlines and speeds up the implementation of compliance rules.

Takeaways

- Compliance regimens like ISO 27001 and GDPR mandate strong control, transparency, and audit logging of privileged (admin) users and their account sessions.

- Privileged Access Management (PAM) plays both a direct and indirect role in expediting compliance by ensuring that only authorized admin users can set up and manage controls that affect compliance.

Executive Summary of CISO Guide

Chief Information Security Officers (CISOs) frequently handle a portion of their organizations' compliance programs. This makes sense, given how many compliance controls are either based on or identical to cybersecurity controls. Many security factors contribute to compliance. However, PAM emerges as one of the most important security processes to help speed up and simplify compliance:

- **GDPR** - GDPR compliance involves tracking administrative access control for systems that manage private personal data. PAM supports this requirement by giving the CISO strong control over admin access to systems essential for maintaining data privacy. It also provides the basis for a streamlined internal audit for GDPR compliance.

- **ISO 27001** - PAM helps speed up compliance with ISO 27001 controls on both a direct and indirect basis, e.g. controlling access to privileged accounts (Section A.9), physical and environmental security (Section A.11), and supplier relationships (Section A.15). PAM indirectly supports information security policies and compliance with internal requirements (Sections A.5 and A.18).

- **HIPAA, SOX, PCI, etc.** – These major compliance schemes all contain requirements dictating control and auditability of privileged account access and sessions. A PAM solution can expedite compliance.

- **Deployment, Cost, Adoption and Adaptability** – The WALLIX PAM solution enables an organization to overcome major obstacles to compliance: Agentless architecture makes the solution easy to deploy and modify as regulations change. Its uncomplicated nature keeps the cost of PAM low and IT employee productivity high. Automated and intuitive, WALLIX avoids complex PAM processes and rules that may otherwise get ignored over time.

Compliance Requirements Facing the CISO

The CISO usually finds him or herself with some responsibility for compliance, even if there is a dedicated compliance officer at the organization, as security and compliance are closely connected. Conveniently, controls devised for cybersecurity also enable compliance. Examples include:

- Data protection countermeasures used to comply with laws like GDPR which mandate protection of consumer identities.
- Access controls created for security but used to comply with frameworks like ISO 27001 and PCI-DSS.
- Backup and disaster recovery policies that align with data retention compliance rules.

Takeaways

- CISOs are tasked with compliance because controls devised for cybersecurity also enable compliance.

- The challenge for the CISO is to support compliance without overburdening the inevitably limited resources available for cybersecurity work.

- A best practice is to identify core cybersecurity tools and policies that can flexibly support multiple compliance regimens.

The challenge for the CISO is to support compliance without overburdening the inevitably limited resources available for cybersecurity work. Meeting this challenge involves the effective use of people, processes, and tooling. All must work together. No single element can do it all.

However, the integration and orchestration of tooling can help. Trying to map multiple point solutions to an ever-shifting set of compliance requirements will likely be a frustrating, inefficient exercise. A recommended best practice is to identify core cybersecurity tools and policies that can flexibly support multiple compliance regimens. At that point, it becomes possible to map these root cybersecurity capabilities to compliance rules. Table 1 offers a simple example of this kind of mapping process.

Cybersecurity Capability	Includes:	Relationship to compliance	Maps to:
Data protection	• Firewalls • Encryption • Access controls • Privileged access controls	Supports compliance rules that mandate data protection for purposes of privacy and financial transaction integrity, etc.	HIPPA ISO27001 GDPR PCI-DSS
Data retention	• Data storage policies • Backup and recovery	Supports compliance rules mandating retention of data.	SOX
Identity management and privileged access controls	• Identity management systems • Privileged Access Management (PAM) solutions	Needed for compliance rules that require data privacy, transaction integrity, and confidentiality, provable "hardening" of key systems, etc.	HIPPA ISO27001 GDPR SOX PCI-DSS

Table 1 • Mapping cybersecurity capabilities to compliance regulations

PAM is at the Root of Effective, Streamlined Compliance

PAM comprises solutions and processes that enable IT departments to manage and track the activities of all "privileged users." A privileged user has administrative access that enables him or her to oversee critical systems and data, e.g. setting up and deleting accounts on an email server. Like any privilege, "root" privileges should only be extended to trusted people. They should also be revocable.

Accidental or deliberate misuse of privileged access is a serious threat affecting cybersecurity as well as compliance. Given that virtually every information system and device play a role in compliance, control over their administration is essential to being compliant. A malicious actor who successfully impersonates a privileged user can easily undermine compliance.

Takeaways

- PAM enables IT departments to manage and track the activities of all "privileged users," who use administrative access to oversee critical systems and data.

- PAM can and should be at the heart of security policies that support compliance.

- Many compliance rules, even ones not dealing with access management, are rooted in PAM.

As a result, PAM can and should be at the heart of security policies that support compliance. It offers streamlined management of security controls that drive compliance. To put the issue fully into perspective, it's important to understand that a privileged user can be almost anyone or anything. A PAM solution governs privileged access by employees, contractors, and employees of third-party vendors, as well as automated systems both inside and outside the enterprise. Table 2 explains how PAM serves as the root solution for compliance with a variety of important regulations.

Compliance Rule	Requires	PAM's Role at the Root
GDPR: Designing and building privacy into business processes	Business processes must embody GDPR rules about privacy, including notification, pseudonymisation, right to access, right to erasure, etc.	PAM supports the integrity of GDPR by ensuring that only authorized users can embed privacy rules in processes.
GDPR: Appointment of data controller	GDPR compliant organizations have a data controller who is personally responsible for overseeing privacy compliance.	PAM gives the data controller a unified view of the administrative actions that define and enforce security policies mapping to GDPR rules.
GDPR: Data Protection Impact Assessments	Data controllers must perform and report on a data protection impact assessment when there are specific risks expected to occur to the rights and freedoms of "data subjects", those individuals whose data is being collected.	Using PAM discovery tools, the data controller can map the topology of privileged accounts as they relate to compliance with data protection, i.e. risks
ISO 27001: A.9.4.3 Password management system	Control: *"Password management systems shall be interactive and shall ensure quality passwords."*	A PAM solution with a password vault is able to define and enforce password policies related to privileged access.
ISO 27001: A.9.2.2 User access provisioning	Control: *"A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services."*	The PAM solution can grant or revoke privileged access rights to critical systems
ISO 27001: A.9.2.3 Management of privileged access rights	Control: *"The allocation and use of privileged access rights shall be restricted and controlled."*	The PAM solution restricts and controls privileged access rights.

Table 2 • How PAM serves as the root of compliance with regulations in ISO 27001 and GDPR

GDPR and How PAM Speeds Up Compliance

The European Union's (EU's) new General Data Protection Regulation (GDPR) goes into effect May 25, 2018, replacing earlier EU data privacy rules. GDPR simplifies but also tightens consumer privacy protections while increasing penalties for violations.

The New Privacy Rules

The changes made to personal data privacy rules are extensive.

- Even non-EU corporations are bound by GDPR if they handle private EU citizen data.
- Privacy has to be built into business processes.
- Organizations with more than 250 employees must appoint a Data Protection Officer.
- EU citizens must give valid, explicit consent to have their personal data collected, and reserve the "right to erasure" and data portability.
- Data breaches must be disclosed to affected individuals within 72 hours.

GDPR bears on IT and cybersecurity practices, including data management and protection practices, software development, and system administration. With GDPR, privacy is now part of almost every conceivable area of IT - affecting how IT and security teams operate and communicate.

Takeaways

- GDPR affects IT and cybersecurity practices, including data management and protection practices, software development, and system administration.

- PAM supports GDPR by managing and monitoring the users who are authorized to access or administer systems that affect data privacy and protection.

GDPR bears on IT and cybersecurity practices, including data management and protection practices, software development, and system administration. With GDPR, privacy is now part of almost every conceivable area of IT—affecting how IT and security teams operate and communicate.

GDPR and PAM

Complying with GDPR means tracking administrative access control for systems that manage personal data, e.g. managing and monitoring how multiple admins manage and protect data across multiple EU territories for an international business. PAM speeds up meeting GDPR requirements by providing the basis for a streamlined internal audit for GDPR compliance. A PAM solution can show, for example, which roles in an organization are allowed to modify data protection policies.

A PAM solution presents businesses with a more efficient way to manage privileged users than is possible with ad-hoc, semi-manual approaches. For instance, if a privileged user has access to or manages private citizen information, GDPR requires that there be adequate traceability and control over that access. It's possible that an organization could have a privileged user with access to a system containing private information about EU citizens but without transparent access logs. Without the automation and centralized control of a PAM solution, the organization isn't able to record operations realized by this privileged user in sensitive systems, in violation with GDPR requirements.

PAM solutions can also facilitate fast adoption of the new "Privacy by Design" intentions of GDPR. IT managers and security administrators can use the PAM solution to define and enforce controls that make "Privacy by Design" work. It can monitor the privileged account sessions that comprise "Privacy by Design" and alert admins to non-compliant activity.

PAM and ISO 27001 Compliance

ISO 27001, published by the International Standards Organization (ISO), is a set of standards that help organizations create and maintain effective information security. It's based on the premise of continual improvement. As a control framework for virtually every aspect of information security, it contains specifications for developing an information security management system (ISMS).

The ISMS

An ISMS is a framework of policies and procedures aimed at building strong information risk management processes. It includes legal, physical, and technical controls involved in cybersecurity. ISO 27001 doesn't mandate any particular control, but it offers a controls checklist. Each organization must figure out its own best way to comply with the standard and gain certification from the ISO.

Takeaways

- ISO 27001 is a control framework for virtually every aspect of information security.
- A PAM solution enables rapid ISO 27001 implementation through secure, centralized, and streamlined authorization and monitoring of all privileged users connected to ISO 27001 controls.

PAM and ISO 27001

PAM helps speed up compliance with ISO 27001 controls on both a direct and indirect basis, e.g.:

- Direct: Access to privileged accounts comes up specifically in the controls described in Section A.9 of the standard.
- Direct: PAM figures into Section A.11 (Physical and environmental security) and Section A.15 (Supplier relationships).
- Indirect: Managing privileged access indirectly factors into Section A.5 (Information security policies), Section A.16 (Information security management), and Section A.18 (Compliance with internal requirements).

A PAM solution enables rapid ISO 27001 implementation through secure, centralized, and streamlined authorization and monitoring of all privileged users connected to ISO 27001 controls. Specifically, a PAM solution:

- Grants privileges to users only for systems on which they are authorized.
- Grants access only when it's needed and revokes access when the need expires.
- Avoids the need for privileged users to have or need local/direct system passwords.
- Centrally and quickly manages access over a disparate set of heterogeneous systems.
- Creates an unalterable audit trail of any privileged operation.

Other Compliance Regimens and PAM

PAM factors into most major compliance regimens, including HIPAA, Sarbanes Oxley (SOX), and the payment card industry's PCI-DSS standards. As is the case with GDPR and ISO 27001, PAM responds to a critical component of these control sets. Privileged Access Management also indirectly supports other controls by ensuring integrity and transparency on the administrative side.

PAM and HIPAA

PAM solutions enable healthcare IT administrators to control access to systems that manage confidential patient electronic protected health information (EPHI). They define and enforce policies to prevent access to records by those who are not authenticated, authorized, and approved.

For example, HIPAA mandates that an organization, *"Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information and to prevent those workforce members who do not have access from obtaining access to electronic protected health information."* A PAM solution creates administrative user profiles and group profiles with specific EPHI access privileges.

Takeaways

- PAM factors into virtually every compliance regimen, including HIPAA, Sarbanes Oxley (SOX), and the payment card industry's PCI-DSS standards.
- For HIPAA, PAM manages and monitors admin users who can access medical records.
- SOX General IT Controls rely on PAM to ensure that only authorized users can manage controls over financial reporting.
- With PCI-DSS, PAM is at the heart of implementing rules like *"Implement Strong Access Control Measures."*

PAM and SOX

Several SOX IT General Controls are based on access management, e.g. if the configuration of the General Ledger application is part of an IT General Control, then knowing who did the configuring (to an auditable extent) is essential for maintaining strong controls. The privileged user who configures the General Ledger executes a control over financial reporting. For SOX compliance, it's imperative to document and verify who the privileged users are, what their privileges allow them to do—and provide an audit log of their privileged account sessions when required.

PCI-DSS and PAM

Companies that handle credit card transactions must comply with strict security controls under the Payment Card Industry (PCI)-DSS Requirements. The requirements include rules such as *"Build and Maintain a Secure Network," "Implement Strong Access Control Measures," "Regularly Monitor and Test Networks,"* and *"Maintain an Information Security Policy."*

As with SOX and HIPAA, PAM is at the heart of realizing these security objectives. Without effective, efficient control over PAM, it would be nearly impossible to comply with PCI-DSS. An organization in that scenario would not have sufficient knowledge or control over who was accessing the administrative back ends of systems critical to compliance.

Anticipating Future Regulations

Regulations seldom remain constant. As technologies and industries evolve, there will inevitably be changes in compliance rules and the cybersecurity controls that support them. Most compliance schemes assume that the organization will adapt to changes in regulations over time. With some frameworks, like ISO 27001, the expectation of change is built into the model itself, stating that an ISO-certified organization will establish a process of continuous improvement.

A PAM solution can make a difference in how well an organization adapts to inevitable compliance changes. If the solution is difficult and time-consuming to implement and modify, it will not adapt well. Similarly, a solution that is overly complex to use will likely face low adoption. It may even get ignored over time opening the business up to vulnerabilities or even fines for non-compliance. The best PAM solutions for compliance are therefore ones that offer flexible, low-friction deployment and intuitive usability.

Takeaways

- PAM solutions can provide flexibility that enables an organization to adapt to unknown future rules.
- PAM facilitates adaptability through a centralized locus of control for privileged access.

PAM facilitates adaptability through centralized control of privileged access. With the WALLIX Access Manager, privileged users never actually log into the systems they are administering. Instead, they log into the Access Manager, which stores their credentials. As rules change, any modifications to privileged access can be done through this single interface regardless of how many actual systems are affected.

The WALLIX Bastion offers an agentless architecture that enables rapid scaling and easy PAM configuration changes as a business grows. The WALLIX solution is known for its ease of use, which translates into rapid, widespread adoption. Financially, WALLIX offers low PAM costs that drive high IT staff productivity.

A PAM solution can also provide reporting and analysis of privileged account access, used in determining how to implement changes in compliance rules. The WALLIX Session Manager records privileged account sessions for use in incident response, audit, and, importantly, as proof of compliance with any number of security regulations.

Conclusion

Cybersecurity controls are critical to compliance. For this reason, CISOs find themselves tasked with compliance duties. Of the many security processes and controls connected to compliance, management of privileged access is arguably the most important. PAM is at the root of the vast majority of compliance measures, either directly or indirectly. Sound management of privileged users enables economical, effective and adaptable compliance.

PAM can drive faster, more cost-effective compliance with GDPR rules, ISO 27001 controls, HIPAA, SOX, PCI-DSS, and many others. CISOs who shoulder compliance obligations are well advised to investigate the role of PAM in their organizations' compliance programs.

WALLiX

TRACE, AUDIT & TRUST

WALLIX Group is a cybersecurity software vendor dedicated to defending and fostering organizations' success and renown against the cyberthreats they are facing. For over a decade, WALLIX has strived to protect companies, public organizations, as well as service providers' most critical IT and strategic assets against data breaches, making it the European expert in Privileged Access Management.

As digitalization impacts companies' IT security and data integrity worldwide, it poses an even greater challenge if the data involved is highly sensitive. The recent regulatory changes in Europe (NIS/GDPR) and in the United States (NERC CIP/Cyber Security Directorate) urge companies belonging to sensitive sectors to place cybersecurity at the heart of their activity.

In response to these challenges, WALLIX created a bastion designed to secure organizations' core assets while adapting to their daily operational duties: WALLIX Bastion. The WALLIX bastion accompanies more than 100 operators in sensitive sectors to conform with regulations and over 400 organizations in the protection of their critical assets, securing the access to more than 100,000 resources throughout Europe and the MEA region. It was also the first government-certified solution in the market.

WALLIX partners with a trained and certified network of over 90 resellers and distributors that help guarantee effective deployment and user adoption.

WALLIX is the first European cybersecurity software editor to be publicly traded and can be found on EuroNext under the code ALLIX. As one of the leaders of the PAM market, major players trust WALLIX to secure access to their data: Danagas, Dassault Aviation, Gulf Air, Maroc Telecom, McDonald's, and Michelin are among them.

WALLIX is the founding member of Hexatrust. The WALLIX bastion was elected "Best Buy" by SC Magazine and awarded at the 2016 Computing Security Awards, BPI Excellence, and Pôle Systematic.

Twitter: @wallixcom
More information on: www.wallix.com

OFFICES & LOCAL REPRESENTATIONS

WALLIX FRANCE (HQ)

http://www.wallix.com/fr
Email : sales@wallix.com
250 bis, rue du Faubourg Saint-Honoré
75017 Paris - FRANCE
Tél. : +33 (0)1 53 42 12 90
Fax : +33 (0)1 43 87 68 38

WALLIX UK

http://www.wallix.co.uk
Email: ukinfo@wallix.com
1 Farnham Rd, Guildford, Surrey,
GU2 4RG,UK
Office: +44 (0)1483 549 944

WALLIX DEUTSCHLAND

http://www.wallix.de
Email: deinfo@wallix.co
Landsberger Str. 398
81241 München
Phone: +49 89 716771910

WALLIX USA (HQ)

http://www.wallix.com
Email: usinfo@wallix.com
World Financial District, 60 Broad Street
Suite 3502, New York, NY 10004 - USA
Phone: +1 781-569-6634

WALLIX RUSSIA & CIS

http://www.wallix.com/ru
Email: wallix@it-bastion.com
ООО «ИТ БАСТИОН»
107023, Россия, Москва,
ул. Большая Семеновская, 45
Тел.: +7 (495) 225-48-10

WALLIX ASIA PACIFIC

(Bizsecure Asia Pacific Pte Ltd)
Email: contact@bizsecure-apac.com
8 Ubi Road 2, Zervex 07-10
Singapore 408538
Tel: +65-6333 9077 - Fax: +65-6339 8836

WALLIX AFRICA

SYSCAS (Systems Cabling & Security)
Email: sales@wallix.com
Angré 7ème Tranche Cocody
06 BP 2517 Abidjan 06
CÔTE D'IVOIRE
Tél. : (+225) 22 50 81 90

www.wallix.com