The similarities in Privileged Access Management (PAM) requirements

WALLIX | 2018

WALLIX
TRACE, AUDIT & TRUST

GDPR *vs* ISO

The similarities in Privileged Access Management (PAM) requirements

ABSTRACT

This mapping table aims to highlight the similarities in Privileged Access Management (PAM) requirements that exist between the General Data Protection Regulation (GDPR) and the international standard ISO/IEC 27001:2013. It should help readers understand how a ubiquitous privileged access management solution can be used to answer several compliance regulations without disrupting users' and administrators' daily activities. **This mapping table distinguishes the direct and indirect values brought by PAM to help companies comply with both these regulations.**

WALLIX

TRACE, AUDIT & TRUST

GDPR		ISO/IEC 27001:2013		Privileged Access Management
Article	Note	Section	Note	Added Value
5 🟦	These subsections specify that personal data must be: accurate and kept up to date (1d), and processed securely to protect their **integrity and confidentiality** (1f).	A.5 A.6 A.9 A.11 A.12 A.15 A.16 A.18 🟦 ⬛	A majority of controls covered in ISO 27001 meet the requirement of that article as the standard aims to anticipate many of the norms and regulations in place.	PAM plays a critical role in both those scenarios because it reinforces access to critical data and gives super admins the complete visibility over each individual privileged user and their session, including what they do, when, and how. 🟦 ⬛
15 🟦	Under GDPR, individuals have a Right of access over their data. For example, they can request information about **who accesses or will access their data and where** they will be used (1c).	A.6 A.9 A.12 🟦 ⬛	Sections 6, 9 and 12 of ISO 27007 cover three key elements of GDPR's Article 15 because they can provide individuals with information about how their personal data is processed and by whom.	A PAM solution provides super-administrators with a complete visibility over privileged users from the moment the log into a target system; it can list all privileged users according to their rights, grant or revoke access, monitor and record session logs and activities, etc. This visibility can help controllers answer GDPR's Right of access. 🟦 ⬛
24 🟦	The controller and processor in charge of controlling the processing of personal data must **ensure and provide proof of data security** according to state-of-art policies.	A.5 A.6 A.9 A.12 A.15 🟦 ⬛	ISO 27001 largely covers GDPR's Article 24, from ensuring that security policies and roles are defined and in place, to reinforcing access controls.	PAM helps define accurate and thorough security policies by helping super-administrators segregate duties, defining access rights and role allocation. It also reinforces personal data security through the control of access and sessions, and can provide feasible proofs of data security. 🟦 ⬛
25 🟦	To guarantee an optimal level of **data protection by design and by default**, GDPR requires that appropriate technical and organizational measures be undertaken (2) and justified (3).	A.5 A.6 A.9 A.12 A.15 🟦 ⬛	ISO 27001 identifies several controls that answer Article 25 of the GDPR, some of which particularly deal with access and activity control of internal and external parties.	A PAM solution helps define and implement the security policies identified by organizations to comply with GDPR and ISO 27001 by securing all privileged access and sessions, offering controllers password encryption and management, as well as a centralized view of all accounts, users, roles, and sessions in real-time and after an event has occurred through session recording. 🟦 ⬛

Legend:

🟦 Direct need for PAM

⬛ Indirect need for PAM

GDPR		ISO/IEC 27001:2013		Privileged Access Management
Article	Note	Section	Note	Added Value
28	Where data processing involves the intervention of third parties, the data controller has the responsibility to ensure and justify that **all third parties follow GDPR rules** to secure data protection.	A.9 A.15 A.18	Controls A.15 and A.18 of ISO 27001 are dedicated to controlling supplier relationships to ensure information security, and to confirming that companies are compliant with internal requirements. Control A.9 identifies specific security measures that help organizations reach that goal.	The Session Manager module of a PAM solution records all activity logs generated by external parties and enables super-administrators to have a full view of third parties' screens in real-time as if they were in front of the computer. These features can spot and alert fraudulent activities, terminate the sessions automatically or manually, and provide post-mortem proof for audit reports of who did what, when, and how. The PAM solution also ensures that third parties' actions and access are limited to the scope of their mission.
29	GDPR specifically requires that processors **solely access and process the data they need** according the controller's instructions.	A.5 A.9 A.18	Controls A.5 and A.18 of ISO 27001 help the controller define the organizations' security policies. Control A.9, Access Controls, deals with the implementation of this process.	A PAM solution allows controllers to define specific access rules according to each privileged user's rights and gives them the possibly to create different clusters for each privilege and access.
30	All controllers must **keep a detailed track record of all processing** activities under their responsibility (1&2).	A.6 A.9 A.15	Control A.6 helps define a number of security policies to put in place which can give controllers the visibility they need over their users, particularly through the segregation of duties. Controls A.9 and A.15, addressing Access Controls and Supplier Relationships provide a feasible way for them to implement those policies.	From the moment privileged users log into the target systems, their activity is recorded by the PAM solution and can be reviewed in various forms (logs, video, screenshots, etc.). PAM can integrate completely with other cybersecurity solutions such as SIEM to enhance the monitoring of activities and provide a complete security cycle, from high traceability to event alert and reporting.

WALLIX
TRACE, AUDIT & TRUST

GDPR		ISO/IEC 27001:2013		Privileged Access Management
Article	Note	Section	Note	Added Value
32	GDPR calls for an evaluation of security **risks** and for the implementation of strict policies to guarantee data **availability** while maintaining **integrity and confidentiality**, and to achieve **resilience** in the event of an incident.	A.5 A.6 A.9 A.16 A.18	Several controls required by ISO 27001 help answer Article 32. They enable organizations to address and maintain a holistic security cycle, from the definition of accurate policies to their implementation and evaluation.	A PAM solution helps achieve these controls through four main elements: a password vault securing access with encrypted passwords, session management and monitoring, password management features enhancing access controls, and access management enforcing the principles of least privileged though clusters. A PAM solution should also easily integrate with other security technologies to fit in a broader cybersecurity ecosystem.
33	Personal **data breaches must be notified** to the supervisory authorities within 72 hours and without delay. .	A.16	Control 16 of ISO 27001 deals with the management of security incidents and give organizations tools to comply with Article 33	A PAM solution provides security managers with accurate information about privileged account sessions and offers instant reporting on any administrative sessions that takes place on targeted systems which can give security managers a working narrative of the incident, helping controllers meet Article 33 of the GDPR.
35	Before going through data processing, the controller must **assess** the potential security risk and impact of the data processing on information confidentiality and integrity.	A.6	Control A.6 helps define a number of security policies which can give controllers complete visibility over their users. Having complete visibility over data processing provides controllers with some valuable information which can be used to assess data processing' security risks and impacts.	PAM provides administrators with the means to create, adjust, or delete fine-grained groups of users and sub-users. It helps administrators have high visibility over the number of users within their system and allocate roles in a fluid manner. At the same time, administrators can directly assign users the right level of privilege from a central point of command, thereby allowing them respond to the principle of least privilege and segregate duties appropriately. With each role and privilege clearly defined, PAM allows controllers to assess the risk linked to data processing while mitigating the risk of unauthorized or negligent activity within organizations' core network.

GDPR		ISO/IEC 27001:2013		Privileged Access Management
Article	Note	Section	Note	Added Value
40	Supervisory authorities are expected to apply security best practices and lay out **codes of conduct** to ensure the proper application of GDPR.	A.5 A.6 A.18	Controls A.5 and A.6 help define thorough organization and policies for information security. To comply with Article 40, the codes of conduct laid out by supervisory authorities can and should also be determined by internal security requirements and current regulations (A.18).	PAM help security managers define and implement cybersecurity policies and procedures. Setting up a PAM solution requires administrators to create, adjust, or delete fine-grained groups of users and sub-users, which gives them visibility over roles and access rights. It also gives them the ability to segregate duties to respond to the principle of least privilege. These elements are key to respond to Article 40.
58	Independent public authorities in charge of monitoring GDPR compliance to protect European personal data have **the right to access and process any information necessary** for the performance of their task (1).	A.6 A.9	While independent public authorities should have the right to access and process personal data, controllers should have a visibility over which data they are accessing and processing, what they are doing, how, and when according to best practices for cybersecurity.	A PAM solution can restrict the access of independent public authorities and allow them to specifically process and view the information they need, diminishing the risk of negligence and human errors. PAM's Session Manager module can also provide a track record of the activities that have been done on the systems, offering an additional layer of security in case of incident.
59	Supervisory authorities must produce **an annual report of all of their activities** (infringement types, security measures taken to strengthen data protection, etc.).	A.16	Complying with Article 59 of GDPR requires to ensure the management of information security incident, described in ISO 27001's Control A.16. Answering the objectives of this control will produce the necessary information for organizations to write their activity reports.	PAM provides security managers with accurate information about privileged account sessions and offers instant reporting on any administrative sessions that takes place on targeted systems, elements which can help produce the annual activities report required by Article 59.

This mapping table does not constitute as legal advice for meeting the European General Data Protection Regulation (GDPR).

WALLIX
TRACE, AUDIT & TRUST

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