Essential privileged access management controls to align with DORA compliance requirements

ManageEngine
PAM360

The Digital Operational Resilience Act (DORA) (Regulation (EU) 2022/2554 of the European Parliament and of the Council), is a regulation passed by the European Parliament to improve the digital resilience of the financial sector and integrate resilience into broader operational frameworks.

The act aims to address the systemic high risk arising from high levels of interconnectedness across financial entities, financial markets, and financial market infrastructures, and particularly the interdependencies of their ICT systems. DORA mandates financial organizations to follow its guidelines for governance, detection, protection, containment, prevention, and response to limit ICT related incidents.

Why is PAM important to meet DORA’s compliance requirements?

Privileged access management (PAM) is a crucial tool for financial institutions to meet the requirements of DORA.

PAM provides centralized control, strong authentication, password management, session monitoring, and incident response capabilities. By implementing PAM, organizations can enhance visibility into privileged access, reduce the risk of unauthorized actions, and ensure compliance with DORA’s regulations. PAM’s ability to monitor privileged sessions, detect anomalies, and provide audit trails is essential for demonstrating compliance and protecting against cyber threats.

PAM360, the solution to help you meet PAM-based DORA requirements

ManageEngine PAM360 is a complete privileged access security solution that helps IT teams secure, control, monitor, and audit privileged access across their enterprise routines. It offers comprehensive privileged account and session management controls, Zero Trust-compliant access controls, secrets and entitlements management, application and command controls, and AI/ML-driven, real-time analytics to enhance your enterprise's security posture and compliance. The table below has a summary of the DORA requirements and the corresponding security controls offered by PAM360 to address them.

DORA Article	Relevant PAM controls and best practices	How PAM360 helps
Article 5: Governance and organization	Article 5 pertains to the governance and organizational aspects of digital operational resilience for financial entities. This significantly elevates the importance of PAM within organizations. It shifts PAM from a purely IT concern to a strategic priority requiring board-level oversight and regular review.	PAM360 offers admins high-level visibility, control, and governance over privileged activities across the enterprise. In addition, admins have the options to define user roles, specify appropriate access and privileges tagged to these roles, and distribute this information across all devices and assets that exercise such privileged access rights within the organization. Some access governance controls that PAM360 offers are:

DORA Article	Relevant PAM controls and best practices	How PAM360 helps
Article 5: Governance and organization	The regulation emphasizes a risk-based approach, necessitating more sophisticated monitoring and reporting of privileged access activities. It also places greater scrutiny on third-party PAM solutions, potentially influencing vendor relationships and technology choices.	1. Using PAM360, organizations can set up password request-release workflows. These workflows will mandate an approval mechanism for every access request generated. Users are required to enter a reason for their access request, which is relayed to admins. After that, upon verification, the admin may choose whether to allot access or not. This access provisioning can also be combined with a just-in-time (JIT) condition that lets admins allot time-restricted access to users. The workflow can be combined with app-only access control to enforce a much more granular least privilege security practice. This workflow can further be integrated with all major ITSM tools in the market. With the integration enabled, your admins can now provide secure remote access to the target machines only to authorized technicians without

DORA Article	Relevant PAM controls and best practices	How PAM360 helps
Article 5: Governance and organization		sharing the credentials by validating access requests with appropriate ticket or change IDs. 2. With PAM360's endpoint privilege management capabilities, IT admins can enforce access controls tailored to endpoints and applications. These access controls include allowlisting and blocklisting applications, implementing child process controls, removing admin rights at the endpoint level, provisioning JIT access to applications, and configuring privilege elevation specific to endpoints. 3. PAM360 helps organizations implement the principle of least privilege access through controls like role- and policy-based access control, granting users only the permissions necessary for their tasks. In addition, PAM360 monitors and records privileged sessions, ensuring accountability and bolstering overall security.

DORA Article	Relevant PAM controls and best practices	How PAM360 helps
Article 5: Governance and organization		sharing the credentials by validating access requests with appropriate ticket or change IDs. 2. With PAM360's endpoint privilege management capabilities, IT admins can enforce access controls tailored to endpoints and applications. These access controls include allowlisting and blocklisting applications, implementing child process controls, removing admin rights at the endpoint level, provisioning JIT access to applications, and configuring privilege elevation specific to endpoints. 3. PAM360 helps organizations implement the principle of least privilege access through controls like role- and policy-based access control, granting users only the permissions necessary for their tasks. In addition, PAM360 monitors and records privileged sessions, ensuring accountability and bolstering overall security.

DORA Article	Relevant PAM controls and best practices	How PAM360 helps
Article 5: Governance and organization		4. PAM360 offers JIT privilege elevation that allows temporary access to sensitive servers and workstations, thereby eliminating local admin rights on sensitive endpoints and preventing privilege escalation. 5. PAM360 lets admins enforce a dynamic trust scoring system for privileged users and devices. The trust score is determined based on various customizable factors chosen by you. These factors for users and endpoints include, but are not limited to the number of invalid sign-in attempts, sign-in during non-office hours, allowed IP addresses, firewall status, OS version, allowed browser plug-ins/add-ons, services, etc. Based on these trust scores, admins can create and associate access policies to critical endpoints. These policies will determine if a privileged user is to be given access to a device based on the required trust score for the said

DORA Article	Relevant PAM controls and best practices	How PAM360 helps
Article 5: Governance and organization		device. If the trust score drops, the enforced policy will automatically revoke access based on its specifications.
Article 6: ICT risk management framework	Article 6 necessitates that PAM strategies must align with defined ICT security objectives and risk tolerance levels. The article calls for continuous assessment and management of risks associated with privileged access, including implementing protective measures, detecting anomalous activities, and establishing incident response plans specific to privileged account misuse.	PAM360's dynamic trust scoring capabilities as well as privileged user behavior analytics provide organizations with the ability to implement real-time risk management. Further, with PAM360, organizations can determine what policies and security parameters are most important and prioritize them accordingly. PAM360, through its integrations, helps organizations fit PAM seamlessly into their security framework, understand user behavior to spot anomalies and take the appropriate action, and weave security into their business workflows. Further, PAM360 delivers Zero Trust by design, helping organizations adhere to the principle of least privilege. PAM360 offers organizations the ability to provision time-based access, time-based access

DORA Article	Relevant PAM controls and best practices	How PAM360 helps
Article 6: ICT risk management framework		elevation, ticket ID verification, application and command-level allowlisting, and comprehensive endpoint privilege management, among others.
Article 8 and Article 10: Identification and detection	Articles 8 and 10 emphasize that financial institutions should implement robust systems to proactively detect and identify unusual activities. Additionally, they must invest in sufficient resources and capabilities to continuously monitor user behavior, identify anomalies in ICT systems, and detect potential cyberattacks.	PAM360's audit trails instantly record all events around privileged accounts and key activities, login attempts, and scheduled or completed tasks. This data helps in complying with regular internal audits and forensic investigations, demonstrating who accessed what resource or files, where, when, and why. PAM360 integrates with ManageEngine Log360 UEBA to enhance threat and anomaly detection. Log360 UEBA analyzes audit logs from PAM360 to identify unusual user behavior, using risk scores, anomaly trends, and detailed reports. This integration allows for a unified view of both resource and user audit data, helping admins make informed security decisions.

DORA Article	Relevant PAM controls and best practices	How PAM360 helps
Article 8 and Article 10: Identification and detection		PAM360 also integrates with third-party SIEM tools to offer real-time consolidation and correlation of user activities, assets, and threats to continuously identify and isolate bad actors. Additionally, this integration provides security teams with deeper context and insight on how privileged accounts are distributed, interlinked, and accessed throughout your organization, adding an additional layer of security to your defense strategy.
Article 9: Protection and prevention	Article 9 emphasizes the protection and prevention of ICT systems in financial entities, specifically regarding monitoring, controlling, and securing ICT to mitigate risks. Particularly: • Continuous monitoring and control. • Data protection. • Access control policies.	PAM360's authentication features leave no doors unlocked for inappropriate or unauthorized access. PAM360 provides two-factor authentication through its integration with leading MFA tools and IDPs. Users will have to authenticate through two successive stages to access the PAM360 web interface. Moreover, PAM360 provides a centralized credential vault to consolidate, store, manage, and rotate shared sensitive information, such as passwords,

DORA Article	Relevant PAM controls and best practices	How PAM360 helps
Article 9: Protection and prevention		digital certificates, keys, and proprietary documents associated with processing data. By default, PAM360 encrypts all passwords and other sensitive information using the AES-256 symmetric encryption algorithm and stores only these encrypted data into the password database. Furthermore, all such data undergo dual encryption at both the application and database level. Additionally, PAM360 offers a comprehensive view of all privileged accounts, users, and resources in the organization from a single-central panel. Admins can mandate all privileged sessions to be launched from PAM360, giving them complete control over remote sessions including live monitoring, recording, collaboration, and termination capabilities. Access to data stored in PAM360 is governed by assigned roles, which define the level of privileged

DORA Article	Relevant PAM controls and best practices	How PAM360 helps
Article 9: Protection and prevention		operations a user can perform. This fine-tuned access control system ensures data security by preventing unauthorized access through the PAM360 interface, using role-based access control (RBAC). Further, PAM360's comprehensive fine-grained access control capabilities help organizations gate access to highly sensitive accounts, credentials, and resources. With time-based access controls, real-time risk evaluation, JIT elevation, and endpoint privilege management, PAM360 furnishes the necessary controls to ensure protection of ICT and mitigate risks.
Article 11: Response and recovery **Article 12:** Backup policies and procedures	These articles require financial organizations to implement robust policies that guarantee the continuity of essential business functions and ensure rapid response capabilities. The articles also stresses the need for backup systems to be in place and ready to activate according to	PAM360 offers various disaster recovery options. **Database backups:** When a server fails, users can do a fresh install of PAM360 and restore the database with the help of the backup file and master key in less than 15 minutes. **High availability:** This feature allows regulated entities to run PAM360 in

DORA Article	Relevant PAM controls and best practices	How PAM360 helps
Article 11: Response and recovery **Article 12:** Backup policies and procedures	established protocols.	an active-active setup. **Application scaling:** For enterprises with multiple sites and service providers managing multiple clients, the application scaling design allows them to have multiple application servers, all using a single SQL availability group or cluster or a Cloud RDS on the back end. **Break-glass export:** All secrets or a specific group of secrets can be scheduled to be exported periodically as an encrypted HTML file. Read-only server: PAM360 comes with a read-only (RO) server for the PostgreSQL database. The RO servers function as mirror servers, synchronizing all of the primary server's operations. In the event of the primary server failing, admins can convert any RO server into the primary server and reconfigure all other RO servers to

DORA Article	Relevant PAM controls and best practices	How PAM360 helps
Article 11: Response and recovery **Article 12:** Backup policies and procedures	established protocols.	point to the new primary server. In the event of network connectivity loss or degradation between PAM360 application servers, each application will provide local resiliency by operating independently for days to weeks until the connectivity gets restored. A dedicated RO server can be deployed to handle all API requests and other machine identity-based requests. This will eliminate the need to cater service to both human and non-human entities using a single application.

Source: DORA

Next steps

Ready to try PAM360? Book a free, personalized consultation with one of our experts. Or, take a test drive now and explore PAM360's comprehensive features that can help you meet the stringent requirements of the DORA.

About PAM360

PAM360, ManageEngine's enterprise PAM suite, is a complete privileged access security solution that helps IT teams enforce strict governance on access pathways to critical corporate assets. With a holistic approach to privileged access security, PAM360 caters to core PAM requirements and facilitates contextual integration with multiple other IT management tools, resulting in deeper insights, meaningful inferences, and quicker remedies. More than 5,000 global organizations and over 1 million administrators trust PAM360 with their PAM needs. To learn more about PAM360 and its enterprise-grade capabilities, please visit https://mnge.it/pam360.

Disclaimer: *The complete implementation of DORA requires numerous processes, policies, people, and technology controls.The solutions mentioned above are limited to PAM controls offered by PAM360 to help comply with DORA requirements. Coupled with other appropriate solutions, processes, people controls, and policies, ManageEngine PAM360 can help organizations align with DORA. This material is provided for informational purposes only, and should not be considered as legal advice for DORA compliance. ManageEngine makes no warranties, express, implied, or statutory, as to the information in this material. Please contact your legal advisor to learn how the DORA impacts your organization and what you need to do to comply with the act.*