Implementing Privileged Access Management (PAM) for DORA Compliance

A Practical Framework for Swiss Financial Institutions

keyIT

Why This Framework Matters

The Digital Operational Resilience Act (DORA) is a European regulation that applies to financial institutions within the EU. While Switzerland is not part of the EU, Swiss financial institutions that operate in the European market or have business relationships with EU-based firms must align with DORA to maintain regulatory compatibility.

DORA strengthens ICT risk management requirements, focusing on protecting critical systems, ensuring cybersecurity resilience, and improving oversight of third-party providers. One of the key areas of compliance is Privileged Access Management (PAM)—controlling, monitoring, and securing access to critical systems to prevent breaches, fraud, and operational disruptions.

This framework provides a step-by-step approach for implementing PAM in a way that supports both DORA compliance and FINMA regulations, ensuring:

- Secure and controlled access to critical financial systems.
- Continuous monitoring and audit readiness.
- Governance over third-party IT service providers.

The following roadmap outlines how Swiss financial institutions can implement PAM effectively while staying aligned with both Swiss and EU regulatory expectations.

Phase 1: Initial Assessment and Planning

Define Stakeholders and Responsibilities:

- Identify key stakeholders within the organization, such as CIOs, CISOs, and IT Managers.
- Assign responsibility for compliance and PAM implementation to the appropriate team members.

Conduct Risk Assessment:

- Identify all privileged accounts within the organization, including administrative accounts, service accounts, application accounts, etc.
- Evaluate current access control policies and identify areas of non-compliance with DORA requirements (e.g., access control, incident reporting, third-party risk management).

Select PAM Solution:

- Choose a PAM solution that aligns with the organization's needs and DORA compliance requirements, such as Delinea's Secret Server.

Develop a Roadmap:

- Establish a roadmap for PAM deployment, considering the maturity model.
- Phase 1: Focus on the most critical accounts and systems.
- Phase 2: Expand to other areas like session management, password rotation, and MFA.
- Phase 3: Complete deployment with testing, reporting, and monitoring.

Phase 2: PAM Solution Deployment

Centralize Privileged Account Management:

- Implement centralized vaulting for privileged credentials (e.g., Secret Server), ensuring all privileged credentials are securely stored and managed.

Implementing Privileged Access Management (PAM) for DORA Compliance

A Practical Framework for Swiss Financial Institutions

keyIT

Implement Access Control and Least Privilege Model:

- Ensure that users only have the privileges necessary for their roles.
- Configure access permissions to enforce the least privilege principle across the organization.

Enable Multi-Factor Authentication (MFA):

- Integrate MFA for all privileged accounts to add an additional layer of security.

Session Recording and Auditing:

- Enable session recording and auditing for all privileged sessions, ensuring comprehensive audit trails for compliance with DORA's incident reporting requirements.

Third-Party Access Control:

- Implement strict controls for third-party vendors, ensuring their access is tightly managed and monitored.

Phase 3: Compliance Testing and Validation

Test Privileged Access Security:

- Regularly test the security of privileged access controls, simulating cyberattacks and system failures to ensure resilience and compliance with DORA's resilience testing requirements.

Perform Vulnerability Assessment:

- Perform continuous vulnerability assessments to the PAM solution to ensure there are no weaknesses in the system

Ensure Incident Management Capabilities:

- Verify that the PAM solution enables fast detection, reporting, and remediation of privileged access-related incidents. Conduct regular incident response drills..

Phase 4: Ongoing Monitoring and Reporting

Monitor Privileged Access:

- Continuously monitor privileged access for suspicious activity and ensure real-time alerts are set up for abnormal behavior.

Generate Compliance Reports:

- Set up reporting mechanisms to meet DORA's incident reporting and resilience requirements, generating detailed reports on access activities, vulnerabilities, and incidents.

Ensure Incident Management Capabilities:

- Verify that the PAM solution enables fast detection, reporting, and remediation of privileged access-related incidents. Conduct regular incident response drills..

FIND US
www.keyit.ch

MAIL US
sales@keyit.ch

Implementing Privileged Access Management (PAM) for DORA Compliance

A Practical Framework for Swiss Financial Institutions

keyIT

Conduct Periodic Audits:

- Regularly audit privileged access controls and ensure the organization's PAM solution is up to date with regulatory requirements.

Phase 5: Continuous Improvement

Review and Update PAM Policies:

- Regularly review PAM policies and procedures to ensure they align with evolving DORA requirements and industry best practices.

Training and Awareness:

- Conduct training for IT staff and end-users on the secure use of privileged accounts and access management.

Evaluate Solution Scalability:

- Ensure that the PAM solution can scale as the organization grows and that new systems or services are integrated securely.

Key Takeaways

- Privileged access security is a regulatory necessity under DORA. While FINMA does not explicitly mandate PAM, it requires financial institutions to implement strict access controls, authentication measures, and logging to protect critical IT assets.
- A structured PAM strategy ensures compliance while reducing operational risks. Organizations that take a phased approach will see faster compliance adoption with minimal business disruption.
- Securing privileged accounts protects financial institutions from breaches, fraud, and third-party risks. This framework provides a clear roadmap to achieving PAM maturity while maintaining compliance.

To learn more about implementing a **Privileged Access Management solution for DORA compliance**, contact us by email at **sales@keyit.ch** or fill out **the form**