ConductorOne

DORA Compliance: Identity Security Best Practices

In recent decades, digital technology has infiltrated even the most basic processes, revolutionizing how businesses operate and interact with their customers. But this increased reliance on technology also exposes organizations to new and evolving cyberthreats, by both private and state actors. For example, IBM estimates that the average cost of a data breach is 4.8 million USD. In response to this growing risk, the European Union introduced the Digital Operational Resilience Act (DORA), a framework designed to strengthen the resilience of the financial sector against external threats by establishing a uniform set of standards for managing IT risks.

Essentially, any institution offering financial services within the EU, along with their third-party service providers, falls under its scope—banks, investment firms, insurance companies, and cryptocurrency service providers. With compliance deadlines rapidly approaching (January 17, 2025), it’s crucial for organizations to understand the main requirements and implications of DORA.

DORA focuses on several key areas:

- **ICT risk management:** Implementing robust risk management frameworks to identify, assess, and mitigate information and communication technology (ICT) risks.
- **ICT-related incident reporting:** Establishing clear procedures for reporting and responding to ICT-related incidents.
- **ICT third-party risk management:** Managing risks associated with outsourcing ICT services to third-party providers.
- **Information sharing:** Promoting collaboration and information sharing among financial entities to enhance collective resilience.
- **Digital operational resilience testing:** Conducting regular testing to assess the effectiveness of ICT risk management and incident response measures.

This article provides an overview of DORA, exploring its key requirements, implications for financial institutions, and practical steps organizations can take to ensure compliance with regards to identity and access management (IAM). While DORA does not mention IAM or identity directly, its requirements do affect IAM practices in general: DORA's requirements touch upon various partial aspects of IAM, including strong customer authentication, access control mechanisms, logging, and incident reporting.

Risk Management: Identity Verification, Access Control, and Continuous Auditing

While risk management in IAM might seem straightforward, many organizations still do not practice it effectively. DORA aims to standardize how organizations design their identity verification and access control systems and audit them.

What DORA Says

Article 9 of DORA mandates that financial entities implement "strong customer authentication" where appropriate and "sound security mechanisms" to protect the confidentiality, integrity, and availability of their IT systems. This includes implementing access control mechanisms to prevent unauthorized access to sensitive data and systems.

Best Practices

The following best practices reduce the risk of unauthorized access to sensitive data:

- **Multi-factor authentication (MFA):** Implement MFA for all users, especially those with privileged access.
- **Zero trust security**: Adopt a zero trust security model, which assumes that no user or device should be inherently trusted. This involves verifying every access request and implementing microsegmentation to limit the impact of a potential breach.
- **Least privilege access:** Enforce the principle of least privilege, granting users only the minimum necessary access rights to perform their duties. These privileges should be reviewed as a user changes roles within the company or is assigned new responsibilities.
- **Role-based access control (RBAC):** Manage and enforce access permissions effectively by assigning access to users based on their role. Individual provisioning of access rights should be limited and automatically deprovisioned when no longer needed.
- **Continuous logging of privileged accounts:** Implement continuous monitoring of privileged accounts to track their activities, including login attempts, access to sensitive data, and changes to system configurations.

Incident Reporting: Logging, Auditing, and Alerting

The previous section covered the continuous logging of privileged accounts. However, to ensure compliance, specific actions must be taken with these logs.

What DORA Says

Article 12 of DORA requires financial entities to “ensure logging of all relevant events” related to their ICT systems and applications. This includes logs of user activity, system events, and security-related events. Furthermore, article 17 of DORA mandates that financial entities report major ICT-related incidents to the authorities, including detailed information about each incident, its impact, and the measures taken to address it.

Best Practices

→ **Incident classification and reporting:** Establish an incident management process to record, classify, and address all major ICT-related incidents and significant cyberthreats. This includes assessing the impact of incidents, analyzing root causes, and promptly notifying clients and relevant authorities.

→ **Regular reviews:** Conduct regular reviews of privileged access rights to ensure they remain aligned with the principle of least privilege and that any dormant or unnecessary accounts are disabled.

→ **Automated alerts:** Configure automated alerts for suspicious activities associated with privileged accounts, such as failed login attempts, access to sensitive data outside of normal working hours, or attempts to escalate privileges.

Third-Party Risk Management: Least Privilege Access, Review, and Reporting

Identity and access management (IAM) tools specialize in enforcing least privilege access. For oversight, review, and reporting, identity governance and administration (IGA) tools are the ideal choice.

What DORA Says

Article 23 of DORA explicitly states that financial entities must “manage ICT third-party risk,” including “access rights” and “preventing unauthorized access” to their information and ICT systems. The same article emphasizes the need for “ongoing due diligence” and “periodic assessments” of ICT third-party service providers.

Best Practices

→ **Automated provisioning and deprovisioning:** Automating these processes ensures timely and accurate management of permissions.

→ **Centralized access management:** Use centralized IAM tools for tracking third-party access across all systems and applications. Centralizing IAM makes it easier to manage and enforce security policies consistently across all applications and systems.

→ **Automated reporting:** Generate automated reports on third-party access, including user activity, permissions, and compliance with security policies.

→ **Regulatory benchmarking:** Benchmark your organization's policies with industry regulations and government mandates (such as GDPR, SOX, DORA, and so on).

Information Sharing: Exchanging Indicators of Compromise and Configuration Tools

This section outlines how financial institutions are required to cooperate and share information related to cyberthreats.

What DORA Says

Article 45 of DORA encourages financial entities to establish "information-sharing arrangements" to exchange cyberthreat information and intelligence, such as indicators of compromise, tactics, techniques, procedures, cybersecurity alerts, and configuration tools. Finally, financial entities are required to notify their competent authorities (such as national banks) of these initiatives.

Best Practices

It's hard to define best practices related to information sharing and identity security, and DORA does not specify how financial institutions should set up information-sharing arrangements. Nevertheless, information sharing should include descriptions of innovative attack vectors related to identity fraud and phishing. In many countries, these practices are inherently facilitated by joint ventures between financial institutions that develop shared identity resolution technologies.
For example, itsme is a solution created through the collaboration of all Belgian banks.

Digital Operations Resilience Testing: Penetration Testing and Disaster Recovery

Digital operational resilience testing is a crucial process that assesses the ability of an organization's ICT systems and processes to withstand, respond to, and recover from disruptions and threats.

What DORA Says

Article 24 of DORA mandates that financial entities establish a "comprehensive digital operational resilience testing programme" that includes a range of assessments and tests to evaluate the effectiveness of their ICT risk management and incident response measures. Threat-led penetration testing (TLPT) should be carried out "in accordance with the TIBER-EU framework." Finally, when disaster does happen, Article 25 of DORA requires financial entities to "implement appropriate ICT backup and recovery arrangements" to ensure business continuity in the event of a disruption. This includes having disaster recovery plans specifically for critical ICT systems, including IAM services.

Best Practices

→ **Penetration testing:** Conduct regular penetration testing (preferably by a third party) of your IAM infrastructure to identify vulnerabilities and weaknesses that could be exploited by attackers. This should include testing authentication mechanisms, access controls, and other security measures.

→ **Red teaming:** Adopt TIBER-EU, a framework developed by the European Central Bank to help organizations in the EU, especially financial institutions, test and improve their cybersecurity resilience.

→ **Vulnerability scanning:** Perform regular vulnerability scans to identify and remediate known security vulnerabilities in your IAM systems and applications.

→ **Disaster recovery planning:** Create a detailed disaster recovery plan for your IAM services, outlining procedures for backup and recovery, failover mechanisms, and communication protocols.

→ **Backup of critical IAM components:** Implement backup and recovery mechanisms for critical IAM components, such as user directories, authentication servers, and access control systems.

→ **Geographic redundancy:** Consider implementing geographic redundancy for your IAM infrastructure to ensure availability even in the event of a regional outage.

Conclusion

In this article, we've outlined various IAM best practices related to the five areas of Europe's Digital Operational Resilience Act: risk management, incident reporting, third-party risk management, information sharing, and resilience testing. If you're looking for a modern identity governance platform, consider ConductorOne. We're on a mission to modernize access controls to reduce standing privileges, boost team productivity, and enforce zero trust with self-service access, just-in-time provisioning, and automated access controls and reviews.

Talk to our team.

Or take a self-guided tour to learn more!

Try ConductorOne now

Get a demo