How ID-ware can support your organisation to comply with DORA

What is DORA?

The DORA (Digital Operational Resilience Act) is a sector-specific EU regulation that entered into force beginning of 2023 and applies since 17 January 2025. It aims at strengthening the IT security of financial entities such as banks, insurance companies and investment firms, making sure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption.

DORA brings harmonisation of the rules relating to operational resilience for the financial sector applying to 20 different types of financial entities as well as Information and Communication Technology (ICT) third-party service providers.

DORA covers five main areas:

1. **ICT Risk Management**
2. **ICT Third-Party Risk Management**
3. **Digital Operational Resilience Testing**
4. **Reporting of ICT-related Incidents**
5. **Exchange of Information & Intelligence on Cyber Threats**

How DORA relates to Physical Identity & Access Management (PIAM)

As DORA should be considered a sector-specific EU legal framework in relation to the NIS2 Directive with regard to financial entities, the provisions of DORA relating to the above mentioned main ICT-related areas shall apply instead of those provided for in the NIS2 Directive.

Therefore, just like NIS2, DORA aims to protect financial entities from identity-based cyberattacks and unauthorised access to information which could of course also be gained physically. The principle is: Only the right people should have access to the right information at the right time.

A secure and auditable PIAM Suite can ensure that physical identities are only able to access the data and systems that they really need to do fulfil their individual role and thus protect critical information.

How ID-ware can support your organisation in reaching DORA compliance

Our Physical Identity & Access Management (PIAM) Suite improves risk management, resilience, auditability and reporting regarding the complete credential and physical access lifecycle.

ICT Risk Management

DORA expects financial entities to set up and document an IT risk management framework and to review it at least once per year.

Our PIAM Suite manages the lifecycle of credentials for employees, visitors and contractors, including physical access authorisations across multiple locations so that it documents every taken step regarding authorisations.

Policy enforcement ensures that only individuals with the right roles can access restricted areas. Due to the automated management of authorisations, e.g. immediate withdrawal of all authorisations across all systems if an employee leaves the company, possible risks are minimised or prevented.

ICT Third-Party Risk Management

The Contractor Management Module of our PIAM Suite supports organisations in complying with DORA’s requirement to monitor all third-party contractual arrangements.

Multiple sites and different contractor companies increase the risk of duplicated or fake identities for organisations, therefore it is important to mitigate such risks both by having centralised control of all contractor activities and their physical access authorisations.

Our Contractor Module enables a clear overview of all contractors and their status as well as access authorisations across all locations of an organisation. Time-bound, role-based physical access authorisations can be issued to minimise risk exposure.

Digital Operational Resilience Testing

To comply with DORA, organisations must perform annual resilience tests to ensure that all systems function as required. While DORA preliminarily focuses on digital resilience, physical infrastructure is tightly coupled to digital assets.

Our robust and reliable PIAM Suite helps to secure this layer, offers highest encryption standards, supports auditability and enhances the overall operational resilience.

Reporting of ICT-related incidents

DORA requires prompt logging of any ICT-related incidents and their reporting to the authorities.

Our PIAM Suite offers comprehensive reports with documented actions steps, automating detailed reporting without manual effort required. Detailed logs and access records are provided.

iDware

Exchange of Information & Intelligence on Cyber Threats

Under DORA, financial organisations are required to share information about cyber threats and incidents with authorities as well as other entities in the financial sector. Goal is to improve situational awareness and collaborate to increase cybersecurity.

Our PIAM Suite helps to reach cyber-physical convergence, i.e. combined physical and cyber security operations to protect your organisation and data. A secure Physical Identity and Access Management (PIAM) is essential to protect IT infrastructure.

In addition, physical access management helps to protect digital assets too. If an incident occurs, the logs of our PIAM Suite and its modules can provide critical insights into who was physically present and may have compromised the system. Due to the automated and comprehensive reporting possibilities of our PIAM Suite, information on threats and incidents can be easily shared with other financial organisations to align on further improving security measures.

Deploying the ID-ware PIAM Suite manages the physical layer mandatory to safeguard the digital resilience for DORA, as it contributes to the enhancement of operational resilience of financial organisations: It increases security, supports risk management and facilitates information exchange on threats and incidents.

About us

ID-ware is a leading global provider of Physical Identity and Access Management (PIAM) solutions.
With over 20 years of experience, we are specialised experts for effective identification and authentication processes to support large-scale organisations.

Our innovative and secure products in connection with our strong principle of long-term partnerships make our customers profit from customised solutions for their complex environments.

☎ Netherlands: +31 70 337 1500
Germany: +49 69 210 8555 60
UK: +44 20 8050 2648

✉ info@id-ware.com