



ENTRUST

Compliance Solutions for DORA, the EU's Digital Operational Resilience Act

Learn about the EU regulation on cyber risk affecting financial institutions and their information and communication technology (ICT) partners – and how Entrust can help.

Overview

As financial organizations embrace digital transformation, they also increase their exposure to rapidly evolving cyber threats. Threat actors are posing greater risks than ever to the financial services sector.

The **Digital Operational Resilience Act** (DORA) is a European Union (EU) regulation that targets how financial institutions and their ICT partners manage cyber risk. It creates a binding oversight framework and establishes technical standards that EU financial entities and their service providers must implement by January 17, 2025, to comply with their DORA requirements. By that time, each EU Member State will begin enforcing compliance. Designated regulators, known as “competent authorities,” can request entities to take specific security measures and remediate known vulnerabilities.

Likewise, non-compliance penalties are severe. For example, ICT service providers deemed “critical” by the European Commission will be supervised by “Lead Overseers.”

ENTRUST'S COMPLIANCE SOLUTIONS

- Our broad portfolio of solutions secures identities, data, networks, applications, and workloads and integrates with a broad partner ecosystem
- Mitigate exposure to data breaches
- Facilitate compliance with data security regulations and stringent auditing and risk-reporting requirements
- Maintain visibility of critical data assets

These organizations can penalize noncompliant providers with fines of up to 1% of their average daily worldwide turnover from the previous business year.

[Learn more at entrust.com](https://www.entrust.com)



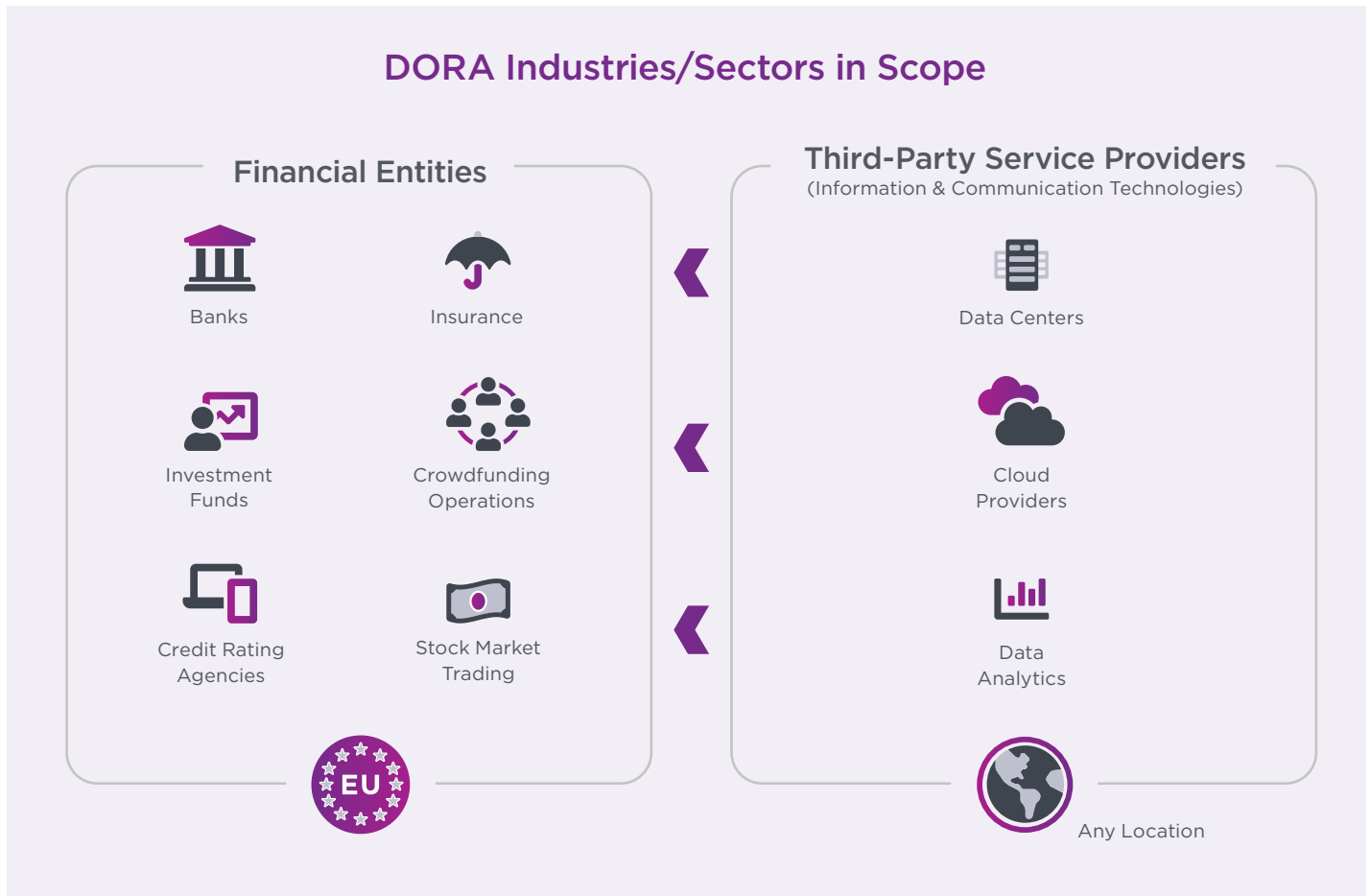
DORA Compliance Solutions

Why is DORA important?

Previously, EU regulations primarily focused on ensuring financial firms had enough capital to cover operational risks and disruptions. Some regulators released guidelines on ICT risk management, but they didn't apply to all entities the same.

Without a unified oversight framework, each EU Member State issued its own requirements. This created a maze of disjointed regulations that cross-border enterprises couldn't easily navigate.

DORA solves this problem with one set of rules for all covered entities regardless of where they operate in the EU. By harmonizing risk management in the financial sector, DORA minimizes confusion and raises the bar for ICT security and business continuity.





DORA Compliance Solutions

Financial entities and third-party providers

DORA applies to a broad range of financial entities and critical third-party providers:

1. Traditional Financial Entities

- Banks
- Investment firms
- Credit institutions
- Insurance companies

2. Non-Traditional Financial Entities:

- Crypto-asset service providers
- Crowdfunding platforms

3. Critical Third-Party Providers:

- ICT service providers (e.g., software vendors, cloud service providers, data center providers)
- Data analytics providers

5 pillars of DORA compliance

DORA's comprehensive framework is structured around five pillars. Each addresses a different aspect of **cyber resilience and risk management**, but in combination, they form the foundation for a strong and secure financial sector.

RISK MANAGEMENT



Business continuity policies and disaster recovery plans as C-level responsibilities

ICT THIRD-PARTY RISK



Critical ICT third parties subject to an EU oversight framework

DIGITAL OPERATIONAL RESILIENCE TESTING



Recommend annually as a minimum include third parties/suppliers

MANDATORY INCIDENT REPORTING



Harmonization across other EU incident reporting frameworks (GDPR, PSD2, NIS2)

VOLUNTARY INCIDENT AND INFORMATION SHARING









Exchange of threat and incidents intelligence








DORA Compliance Solutions

DORA Regulation / Entrust Solution Mapping - EU 2022/2554

| DORA Section | DORA Requirement | Entrust Solutions |
|---|---|---|
| Article 8, Identification | | |
| Paragraph 1 | <p>As part of the ICT risk management framework "... financial entities shall identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions"</p> <p>"Financial entities shall maintain relevant inventories and update them periodically"</p> |  <p>Entrust KeyControl: Build a comprehensive inventory of cryptographic assets (keys, secrets, and digital certificates) and virtual machines.</p> |
| Article 9, Protection and prevention | | |
| Paragraph 2 | <p>"Design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit"</p> |  <p>A combination of Entrust Identity as a Service (ensure confidentiality), Entrust nShield HSMs (protect cryptographic keys), Entrust KeyControl (key and secret management), and Entrust PKI solutions (authentication and digital signatures) can help deliver these requirements on premises or with cloud-based, as-a-service solutions.</p> |
| Article 9, Protection and prevention | | |
| Paragraph 3 Section a | <p>"ensure the security of the means of transfer of data"</p> |  <p>Entrust PKI can provide TLS certificates to ensure integrity of data transfer. Entrust KeyControl can be used for encrypting data in transit. HSMs protect keys in data transfer.</p> |
| Paragraph 3 Section b | <p>"minimise the risk of corruption or loss of data, unauthorised access and technical flaws that may hinder business activity"</p> |  <p>Entrust Identity as a Service can prevent unauthorized access. Entrust PKI (signature), KeyControl (signatures, hashing), nShield HSMs.</p> |
| Paragraph 3 Section c | <p>"prevent the lack of availability, the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data"</p> |  <p>All Entrust products include a resilience/ high-availability capability to ensure minimal disruption of service. Entrust PKI can play a role in ensuring authenticity and availability Entrust Identity, KeyControl, and nShield HSMs can help prevent breaches and loss of data.</p> |
| Paragraph 3 Section d | <p>"ensure that data is protected from risks arising from data management, including poor administration, processing-related risks and human error"</p> |  <p>Entrust CloudControl enables separation of duties, least privilege, and secondary approval mechanisms. Entrust Identity as a Service offers a policy engine to assign roles and control access management.</p> |





DORA Compliance Solutions

| DORA Section | DORA Requirement | Entrust Solutions |
|---|---|---|
| Article 9, Protection and prevention | | |
| Paragraph 4 Section c | “implement policies that limit the physical or logical access to information assets and ICT assets to what is required for legitimate and approved functions and activities only, and establish to that end a set of policies, procedures and controls that address access rights and ensure a sound administration thereof” |  <p>Entrust Identity as a Service, nShield HSMs, and KeyControl provide physical and logical security controls, and encryption, preventing logical access to data. Entrust CloudControl prevents unauthorized logical access to data in virtual environments.</p> |
| Paragraph 4 Section d | “Implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes” |  <p>Entrust Identity, Entrust PKI, and Entrust CloudControl provide strong authentication mechanisms. Entrust nShield HSMs and KeyControl enable you to generate, manage, and protect cryptographic keys.</p> |
| Article 10, Detection | | |
| Paragraph 2 | “Financial entities shall have in place mechanisms to promptly detect anomalous activities. The detection mechanisms “shall enable multiple layers of control, define alert thresholds and criteria to trigger and initiate ICT-related incident response processes, including automatic alert mechanisms for relevant staff in charge of ICT-related incident response.” |  <p>Entrust Identity solutions offer adaptive risk-based access and authentication. They provide added security via contextual authentication driven by adaptive risk-based policy engine to verify users and devices before granting access. Non-intrusive detection of user behavioral and environmental anomalies protects consumers from credential-stealing attacks, impersonation attacks, and computer/session takeover attacks.</p> |
| Article 11, Response and recovery | | |
| Paragraph 6 Section a | “Test the ICT business continuity plans and the ICT response and recovery plans in relation to ICT systems supporting all functions at least yearly, as well as in the event of any substantive changes to ICT systems supporting critical or important functions” |  <p>Entrust KeyControl's distributed architecture simplifies maintenance tasks, reducing the complexity of operations such as upgrades and backup/restore and readily supporting scenario planning activities such as disaster recovery. Vaults can be isolated without facing the scheduling challenge, risk, and unpredictability of taking your entire organization's KMS offline and then back online, thereby lowering the risk of service disruptions.</p> |
| Paragraph 6 Section b | “Test the crisis communication plans established in accordance with Article 14.” “Financial entities...shall include in the testing plans scenarios of cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities necessary to meet the obligations set out in Article 12.” |  <p>All our solutions, including Entrust KeyControl, nShield HSMs, and Entrust Identity, can be deployed on redundant facilities to support switchover from primary to secondary ICT infrastructure.</p> |



DORA Compliance Solutions

| DORA Section | DORA Requirement | Entrust Solutions |
|---|--|---|
| Article 12, Backup policies and procedures, restoration and recovery procedures and methods | | |
| Paragraph 2 | Financial entities shall set up backup systems that can be activated in accordance with the backup policies and procedures, as well as restoration and recovery procedures and methods. The activation of backup systems shall not jeopardize the security of the network and information systems or the availability, authenticity, integrity or confidentiality of data. Testing of the backup procedures and restoration and recovery procedures and methods shall be undertaken periodically. |  <p>All our solutions, including KeyControl, nShield HSMs, and Entrust Identity as a Service, can be deployed on redundant facilities to support switchover from primary to secondary ICT infrastructure. Entrust KeyControl's distributed architecture lends itself to scenario planning exercises such as cyber incidents where individual vaults can be readily switched offline and restored with minimal business impact.</p> |
| Article 24, General requirements for the performance of digital operational resilience testing | | |
| Paragraph 1 | "For the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures, financial entities, other than microenterprises, shall, taking into account the criteria set out in Article 4(2), establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework referred to in Article 6." |  <p>Entrust KeyControl's distributed architecture simplifies maintenance tasks, reducing the complexity of operations such as upgrades and backup/restore and readily supporting scenario planning activities such as disaster recovery. Vaults can be isolated without facing the scheduling challenge, risk, and unpredictability of taking your entire organization's KMS offline and then back online, thereby lowering the risk of service disruptions.</p> |



DORA Compliance Solutions

Strengthen cyber resilience with Entrust

Whether you're a financial entity or an ICT provider, Entrust's portfolio can help you harden your defenses and protect critical infrastructure.

Our solutions include:

- **Hardware security modules (HSMs):**
Entrust nShield HSMs help provide a secure environment for generating, managing, and protecting cryptographic keys, which are crucial for data encryption and secure communications.
- **Cloud security posture management:**
The **Entrust CloudControl** security platform helps protect your hybrid cloud environments by making it easy to identify, remediate, and report on configuration and compliance in one pane of glass.
- **Key and secrets management:**
Key and secrets management is essential to ensuring the confidentiality and integrity of data and financial transactions. **Entrust KeyControl** helps you to manage cryptographic assets throughout their lifecycle, preventing unauthorized access to ICT systems.
- **Identity and access management:**
Entrust Identity as a Service is an intelligent platform that streamlines user authentication, authorization, and access control. Connect with your consumers through secure portals, identity proofing, and more.
- **Public key infrastructure (PKI):**
Entrust PKI helps provide a framework for secure communications and authentication, using digital certificates to verify entities and encrypt data.

Entrust is a proven, expert adviser in security with decades of experience and a wide portfolio of solutions that can help organizations address the requirements of DORA and apply appropriate measures to improve their security posture.

For more information

888.690.2424

+1 952 933 1223

sales@entrust.com

entrust.com

ABOUT ENTRUST CORPORATION

Entrust is an innovative leader in identity-centric security solutions, providing an integrated platform of scalable, AI-enabled security offerings. We enable organizations to safeguard their operations, evolve without compromise, and protect their interactions in an interconnected world – so they can transform their businesses with confidence. Entrust supports customers in 150+ countries and works with a global partner network. We are trusted by the world's most trusted organizations.

Learn more at
entrust.com



Entrust and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.
© 2024 Entrust Corporation. All rights reserved. DS25Q2-dora-compliance-solutions-sb

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223