

SOLUTION BRIEF

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



ENTRUST

SECURING A WORLD IN MOTION



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 have been required to meet since January 17, 2025. EU Member States now actively enforce 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

- The Entrust Cryptographic Security Platform unifies PKI, HSMs, and key, certificate, and secrets lifecycle management in a single trust layer built for crypto-agility and resilience
- Mitigate exposure to data breaches
- Facilitate compliance with data security regulations and stringent auditing and risk reporting requirements
- Maintain visibility and governance across cryptographic assets – keys, secrets, certificates, and the machine identities that depend on them

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

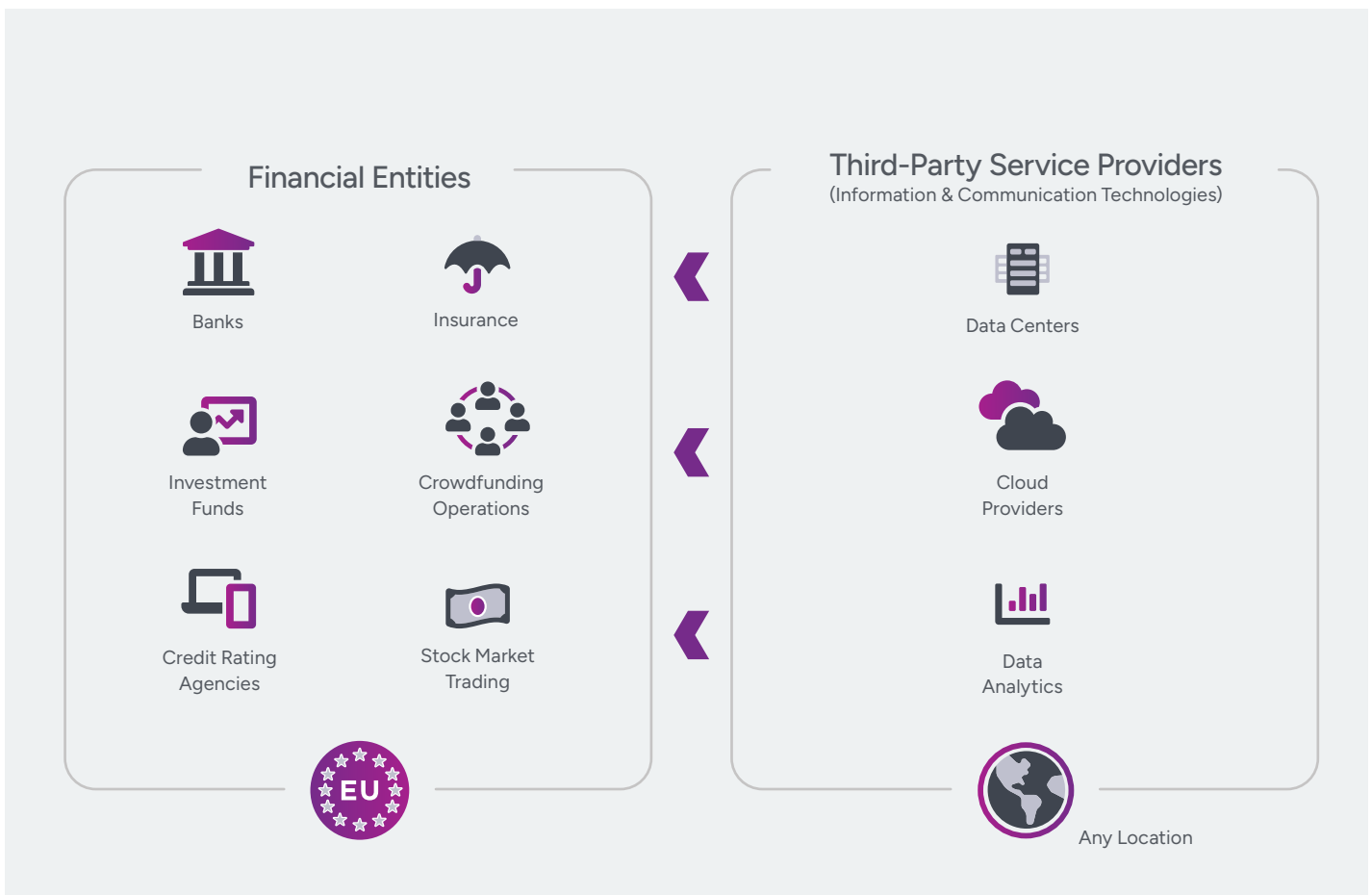


Why is DORA important?

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.



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	ICT THIRD- PARTY RISK	DIGITAL OPERATIONAL RESILIENCE TESTING	MANDATORY INCIDENT REPORTING	VOLUNTARY INCIDENT AND INFORMATION SHARING
				
Business continuity policies and disaster recovery plans as C-level responsibilities	Critical ICT third parties subject to an EU oversight framework	Recommend annually as a minimum include third parties/suppliers	Harmonization across other EU incident reporting frameworks (GDPR, PSD2, NIS2)	Exchange of threat and incidents intelligence



DORA Regulation / Entrust Solution Mapping - EU 2022/2554

DORA Section	DORA Requirement	Entrust Solutions
Article 8, Identification		
Paragraph 1	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" "Financial entities shall maintain relevant inventories and update them periodically"	 Entrust CSP Key Manager: Entrust Cryptographic Security Platform: Discover and inventory cryptographic assets across the enterprise. CSP Compliance Manager provides a unified dashboard with granular policy management and monitoring of keys and secrets across locally or geographically distributed vaults, while CBOM import and export helps build complete inventories and correlate them with discovered assets and dependencies.
Article 9, Protection and prevention		
Paragraph 2	"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"	 The Entrust Cryptographic Security Platform delivers these requirements through a single trust layer: CSP PKI (authentication and digital signatures), Entrust nShield HSMs (hardware root of trust), and CSP Key Manager (key and secrets management) – with Entrust Identity as a Service providing access control. Available on premises or as a cloud-delivered service.
Article 9, Protection and prevention		
Paragraph 3 Section a	"ensure the security of the means of transfer of data"	 Entrust CSP PKI can provide TLS certificates to ensure integrity of data transfer, with automated certificate lifecycle management to prevent outages as certificate lifetimes shrink. Entrust CSP Key Manager can be used for encrypting data in transit. HSMs protect keys in data transfer.
Paragraph 3 Section b	"minimise the risk of corruption or loss of data, unauthorised access and technical flaws that may hinder business activity"	 Entrust Identity as a Service can prevent unauthorized access. Entrust CSP PKI (signature), CSP Key Manager (signatures, hashing), Entrust nShield HSMs.
Paragraph 3 Section c	"prevent the lack of availability, the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data"	 All Entrust solutions include resilience/high-availability capability. Entrust CSP PKI can play a role in ensuring authenticity and availability. Entrust Identity, CSP Key Manager, and nShield HSMs can help prevent breaches and loss of data.
Paragraph 3 Section d	"ensure that data is protected from risks arising from data management, including poor administration, processing-related risks and human error"	 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.

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"	 Entrust Identity as a Service, nShield HSMs, and CSP Key Manager provide physical and logical security controls, and encryption, preventing logical access to data. Entrust CloudControl prevents unauthorized logical access to data in virtual environments.
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"	 Entrust Identity as a Service and Entrust CSP PKI provide strong authentication mechanisms. Entrust nShield HSMs and CSP Key Manager enable you to generate, manage, and protect cryptographic keys.
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."	 Entrust Identity solutions offer adaptive riskbased 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.
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"	 Entrust CSP Key Manager 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 key management service offline and then back online, thereby lowering the risk of service disruptions.
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."	 All our solutions, including CSP Key Manager, Entrust nShield HSMs, and Entrust Identity as a Service, can be deployed on redundant facilities to support switchover. CSP HSM Manager gives you one place to manage and monitor the nShield estate, replacing fragmented tools and manual processes with centralized visibility, remote management, and automation.

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.	 All our solutions, including CSP Key Manager, nShield HSMs, and Entrust Identity as a Service, can be deployed on redundant facilities to support switchover from primary to secondary ICT infrastructure. Entrust CSP Key Manager 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. CSP HSM Manager provides centralized monitoring of the nShield estate to support backup, restoration, and switchover testing.
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.”	 Entrust CSP Key Manager 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 key management service offline and then back online, thereby lowering the risk of service disruptions. CSP Compliance Manager supports the testing program by assessing cryptographic risk posture and enforcing policy across distributed functions, divisions, and teams.
Article 6, ICT risk management framework/requirement text on maintaining and updating the framework		
Paragraph 1	The foundation of the entire ICT Risk Management pillar. It requires financial entities to establish and maintain a sound, comprehensive, and well-documented ICT risk management framework as part of their overall risk management system	 The Entrust Cryptographic Security Platform builds crypto-agility into the foundation with cryptographic inventory, CBOM support, and policy control that help you plan and govern algorithm transitions, including the shift to post-quantum cryptography.

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.
- **Key and secrets management:** Key and secrets management is essential to ensuring the confidentiality and integrity of data and financial transactions. [Entrust CSP Key Manager](#) 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):** Public key infrastructure: Entrust CSP PKI as a Service provides cloud-delivered PKI that establishes trusted identities, secures communications, and automates certificate lifecycle management across users, devices, applications, and infrastructure – built for crypto-agility and post-quantum readiness.

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.

Deploy your way.

CSP as a Service delivers key capabilities in a cloud model with a unified onboarding experience, a single commercial contract, and hosting in the U.S., EU, and UK – supporting data residency requirements for EU financial entities.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.