Recorded Future Intelligence Cloud helps you prepare to implement DORA requirements.

The Digital Operational Resilience Act (DORA) aims to harmonize the various IT security requirements for the covered entities in the financial sector. It entered into force on 16 January 2023 and is applicable from 17 January 2025 onwards.

DORA focuses on digital resilience for covered entities and the information and communication technologies (ICT) that they use:

Risk Management	Incident Reporting	Digital Operational Resilience Testing	Third-Party Risk	Information Sharing

Given that DORA will impact not only financial entities, but also the ICT third-party service providers that they rely on, it's suggested that organizations start preparing for compliance.

How can Recorded Future help?

◎ Gain a complete view of your threat landscape to identify what matters to you

Quickly identify top threat actors of interest, especially targeting your third-parties

Determine most concerning malware based on your company's technologies

- Identify risk with third-party suppliers
- Continually monitor vendors for risk
- Identify vulnerabilities in key products and tools
- Monitor geopolitical activity for risk to your facilities and regions of operation

⇄ Implement security controls and make adjustments as necessary

Understand the technical parameters of malware used in threat actor campaigns to close specific ports

Update block lists with continuously validated IP addresses and domains for command & control (C2), botnet and remote access trojan (RAT) infrastructure

Automatically reset passwords in an identity access management (IAM) system with recently stolen credentials

👥 Mitigate software threats originating from 3rd and 4th party vendors

Enrich vulnerabilities on scanned third-party products with data on weaponization

Dynamic risk scoring for third-parties, updated in real-time

🔄 Detect new threats with context

Receive a notification within minutes of a potential breach impacting a key third-party, such as a database offered for sale

Detect references to your brand and "secret" keywords on ransomware extortion sites to quickly understand the severity of potential leaked documents

- Detect anomalous behavior with threat intelligence in your security tools
- Identify potential risks to ICT tools
- Discover gaps in security controls and identify opportunities for improvement
- Research cyberthreats for to meet incident reporting requirements with real-time intelligence

🕐 Decrease time to respond and report

Equip users with essential information, updated in real time, on their threat landscape

Reduce time spent searching, summarizing, and writing reports by hours

Recorded Future AI answers your questions about threat patterns, implications, and intelligence sources

Contact us to schedule a discussion on how you can get ahead of DORA and protect your business.

Request a demo to see how you can pinpoint, prioritize, and take action on exposed credentials with Recorded Future.