RAPIDRATINGS®

Rapid Guide to DORA 2025

How RapidRatings Helps Banks Meet DORA Regulation
(EU Digital Operational Resilience Act)

Introduction

The European Union's Digital Operational Resilience Act (DORA) establishes a unified framework for managing operational resilience in the financial sector. It mandates that financial institutions, including banks, ensure that their information and communication technology (ICT) systems can withstand, respond to, and recover from cyber threats and operational disruptions. A crucial part of DORA's focus is on the governance of third-party ICT service providers, particularly regarding risk management, oversight, and resilience.

RapidRatings, through its FHR® and risk monitoring solution, can play a key role in helping banks meet DORA's stringent requirements. This document outlines how RapidRatings aligns with the DORA framework and facilitates compliance for financial institutions.

This summary is based on the official EU Digital Operational Resilience Act accessible in full at EU Lex.

Who Needs to Comply with DORA?

DORA applies to a broad range of financial services entities within the EU, including but not limited to:

- Banks and credit institutions
- Payment institutions
- Investment firms
- Insurance and reinsurance companies
- ICT service providers that serve these entities

The regulation mandates that all covered entities implement risk management frameworks that ensure digital operational resilience, particularly regarding their ICT service providers.

Key Takeaway

DORA applies to all financial entities operating in the EU, including ICT third-party providers. RapidRatings' solutions enable banks to align with DORA's requirements by helping them monitor and assess the financial health and resilience of their critical third-party service providers including all of those providing ICT services.

Prominence of Third-Party Risk Oversight in DORA

DORA mandates stringent oversight of third-party ICT providers, placing heavy emphasis on risk management, including financial stability and operational resilience.

Key Requirements (Articles 28-30)

- Due Diligence: Financial institutions must thoroughly assess third-party providers before entering into contracts, including financial viability and operational capacity.
- Ongoing Monitoring: Once engaged, banks must continuously monitor their ICT service providers, ensuring they can maintain service levels, particularly during operational disruptions.
- Risk Mitigation: Contracts with third-party ICT providers should include provisions for termination if the third party is unable to meet financial or operational expectations.

How RapidRatings Helps

- RapidRatings enables financial institutions to assess the financial stability and resilience of their ICT service providers, ensuring compliance with DORA's due diligence and ongoing monitoring requirements.
- RapidRatings' FHR® provides a comprehensive analysis of the financial health of third-party providers, helping banks identify potential risks before and after entering into contracts.

Key Takeaway

DORA requires that banks maintain robust oversight of their third-party ICT providers' financial and operational resilience. RapidRatings provides essential risk analysis and reporting that banks can use to ensure compliance with these requirements.

Financial Condition Analysis

A critical part of DORA's focus is ensuring that banks can continue to operate even when their ICT systems face disruptions or failures. This includes assessing the financial condition of ICT providers, as their financial instability can lead to service failures or risks that disrupt banking operations.

Key Requirements (Articles 32-33)

- **Financial Health Assessments:** Banks must assess the financial health of ICT providers, ensuring they have the resources to remain operational and deliver services under various scenarios.
- **Stress Testing:** Banks must ensure that ICT service providers can handle adverse operational scenarios, including financial distress.

How RapidRatings Helps

RapidRatings offers in-depth financial health assessments, based on the third-parties' financial statements that align with DORA's focus on third-party resilience. Our **financial health rating** offers a detailed view of the financial stability of third-party ICT providers, highlighting key risks such as liquidity issues, debt exposure, and profitability. The FHR® analysis can help banks make informed decisions and reduce the likelihood of engaging high-risk vendors.

Key Takeaway

RapidRatings gives banks a predictive analysis of their ICT providers financial health based on their actual financial statements. Thus ensuring compliance with DORA's financial risk management and stress testing requirements.

Ongoing Monitoring and Incident Response

DORA emphasizes the importance of ongoing monitoring and timely responses to incidents that may arise from third-party ICT providers. This means that banks must be proactive in monitoring the resilience of their service providers to detect and mitigate risks promptly.

Key Requirements (Articles 36-40)

- **Real-Time Monitoring:** Financial institutions must continuously monitor third-party providers for signs of financial or operational distress.
- **Incident Reporting:** Banks must establish mechanisms to report and respond to incidents arising from third-party failures, including disruptions to ICT systems.

How RapidRatings Helps

RapidRatings' financial monitoring and automated alerts provide early warnings when an ICT provider's financial health deteriorates, allowing banks to act quickly and prevent disruptions. With access to accurate financial reports, banks can track changes in financial health and adjust their risk management strategies accordingly.

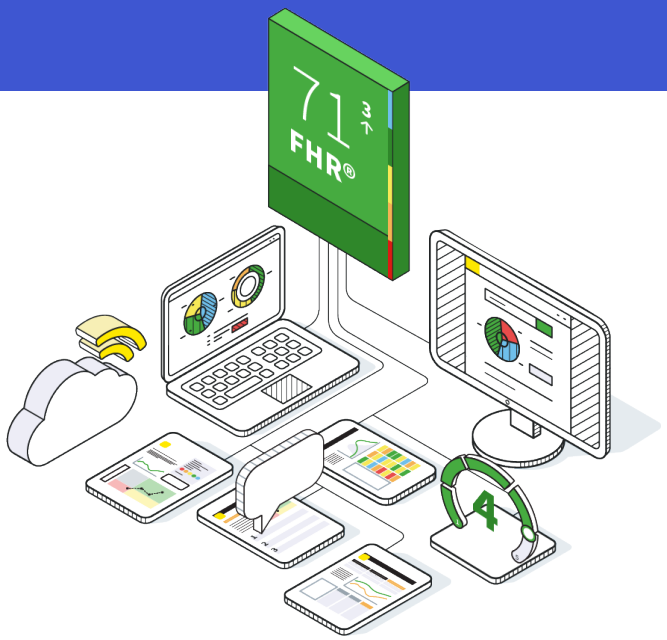
Key Takeaway

RapidRatings supports ongoing monitoring and incident response protocols by offering timely insights into the financial health of critical ICT providers. These insights, along with the robust, detailed reporting, help banks comply with DORA's proactive risk management requirements.

Partnering with RapidRatings for DORA Compliance

RapidRatings is a valuable partner for banks seeking to comply with DORA. Our financial health assessments are based on the analysis of third-party financial statements, providing banks with the critical information they need to ensure their ICT service providers are financially stable and operationally resilient.

How RapidRatings Simplifies Third-Party Risk Assessment



Accurate Financial Health Assessments

We gather and analyze the financial statements of private and public third-parties to produce accurate and predictive ratings, reports, and guidance.

Regulatory Compliance

RapidRatings' solutions are designed to align with DORA's requirements, ensuring that financial institutions can meet their obligations to manage and oversee third-party risk.

Ongoing Monitoring

In-platform customizations allow you to segment, monitor, and manage cohorts of third parties according to criticality and your business needs.

Conclusion

DORA introduces strict requirements for managing the operational resilience of third-party ICT providers, placing a heavy emphasis on financial stability and risk management. RapidRatings helps banks comply with these regulations by providing accurate, predictive assessments of third-party financial health. By partnering with RapidRatings, banks can ensure their third-party relationships are resilient, compliant, and aligned with DORA's requirements.

For more information on how RapidRatings can support your bank in meeting DORA requirements, contact our team at the link below:

Talk to our team

CONTACT OUR TEAM

Solutions@rapidratings.com
+1 646 233-4600

FIND US ONLINE

www.rapidratings.com

RAPIDRATINGS®