REVERSINGLABS

Digital Operational Resilience Act (DORA)

Effective Date: 17 January 2025

This regulation is designed to enhance the overall digital operational resilience of the EU financial sector.

DORA Regulatory Technical Standards **Key Excerpts**	**How Spectra Assure Helps**
Article 16 “Proprietary software and, where feasible, the source code provided by ICT third-party service providers or coming from open-source projects, shall be analysed and tested prior to their deployment in the production environment.”	**Complete Software Analysis:** Spectra Assure helps businesses meet DORA by providing the most comprehensive risk assessment of the entire software application. It analyzes the complete software binary, including proprietary, third-party commercial, and open source components embedded within the package to ensure it is safe before deployment into production.
Article 34 “Implement measures to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware…”	**Broad Risk & Threat Coverage:** Spectra Assure helps detect a wide range of risks and threats required by DORA including: exposed secrets, malware, vulnerabilities, and more.
Article 10 “Track the usage of third-party libraries, including open source, used by ICT services supporting critical or important functions”	**Independent SBOM Generation:** Spectra Assure helps businesses meet DORA by providing the most comprehensive risk assessment of the entire software application. It analyzes the complete software binary, including proprietary, third-party commercial, and open source components to ensure it is safe before deployment into production.

Source: Regulatory Technical Standard on ICT Risk Management Framework