

SOLUTION BRIEF

Contrast Security and **The Digital Operational Resilience Act (DORA)**

The Digital Operational Resilience Act

The Council of the European Union (EU) is comprised of government ministers from each EU country with the authority to create and amend laws and coordinate policies. Regarding IT security, the council adopted the Digital Operational Resilience Act (DORA) in November 2022. The intent of DORA is to provide consistent IT security standards for financial institutions (banks, insurance companies, investment firms) across all EU member states such that the EU financial sector can stay resilient against cyber threats and operational disruption.



REGULATION (EU) 2022/2554

In December 2022, the Digital Operational Resilience Act was published as Regulation (EU) 2022/2554 in the Official Journal of the European Union and became effective on January 16, 2023. This is a binding regulation for all EU members, not simply a directive.

WHAT IS REQUIRED IN DORA REGULATION (EU) 2022/2554?

Described in detail in a [79 page document](#)¹, Article 25 of the regulation outlines the essential elements for testing:

Testing of information and communication technology (ICT) tools and systems

1. The digital operational resilience testing programme referred to in Article 24 shall provide, in accordance with the criteria set out in Article 4(2), for the execution of appropriate tests, such as vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing.
2. Central securities depositories and central counterparties shall perform vulnerability assessments before any deployment or redeployment of new or existing applications and infrastructure components, and ICT services supporting critical or important functions of the financial entity.

¹ REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554>

3. Microenterprises shall perform the tests referred to in paragraph 1 by combining a risk-based approach with a strategic planning of ICT testing, by duly considering the need to maintain a balanced approach between the scale of resources and the time to be allocated to the ICT testing provided for in this Article, on the one hand, and the urgency, type of risk, criticality of information assets and of services provided, as well as any other relevant factor, including the financial entity's ability to take calculated risks, on the other hand.

HOW CONTRAST SECURITY HELPS SUPPORT DORA REGULATION (EU) 2022/2554

Securing custom applications including 3rd party libraries used by EU financial services firms is essential to support this new regulation. Contrast Security supports DORA Article 25 with the Contrast Secure Code Platform in the following ways:

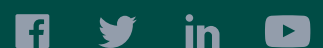
1. Contrast supports the DORA testing requirements of §25(1) for vulnerability assessments and scans, open-source analysis, scanning software solutions, source-code reviews, end-to-end testing, and penetration testing.
2. Contrast's natural pipeline integration make it uniquely capable of meeting the requirements of §25(2) for performing vulnerability assessments of new or existing applications, components, and ICT.
3. Contrast's unlimited scalability, realtime analysis, and high accuracy delivers the capability to achieve an unmatched balance of scale, speed, and effort under §25(3), maximizing security with a minimum of effort.

Contrast Security can help secure your applications taking a key step toward compliance with DORA Regulation (EU) 2022/2554). To schedule a demo and see how this works, contact us here:

<https://www.contrastsecurity.com/request-demo>

Contrast Security provides the industry's most modern and comprehensive Application Security Platform, removing security roadblocks inefficiencies and empowering enterprises to write and release secure application code faster. Embedding code analysis and attack prevention directly into software with instrumentation, the Contrast platform automatically detects vulnerabilities while developers write code, eliminates false positives, and provides context-specific how-to-fix guidance for easy and fast vulnerability remediation. Doing so enables application and development teams to collaborate more effectively and to innovate faster while accelerating digital transformation initiatives. This is why a growing number of the world's largest private and public sector organizations rely on Contrast to secure their applications in development and extend protection in production.

**240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333**



contrastsecurity.com