Contrast SECURITY

Are you ready for DORA?

The European Union's Digital Operational Resilience Act (DORA) will require financial services organizations operating in the European Union to dramatically improve their cybersecurity resiliency.

With the application layer becoming an increasingly common attack vector, it's imperative for FinServ to leverage Runtime Security to better safeguard their applications from vulnerabilities and exploits.

Impacted organizations must comply with DORA by January 17, 2025. Use this checklist to guide your compliance journey.

	Question	Ready?
1	Can you **effectively monitor** third-party risk providers and key contractual provisions?	
2	Do you have the technology and processes in place to conduct **vulnerability assessments and scans** on a regular basis?	
3	Do you have the technology and processes in place to conduct **open-source analyses** on a regular basis?	
4	Do you have the technology and processes in place to conduct **network security assessments** on a regular basis?	
5	Do you have the technology and processes in place to conduct **gap analyses** on a regular basis?	
6	Do you have the technology and processes in place to conduct **source code reviews** on a regular basis?	
7	Do you have the technology and processes in place to conduct **scenario-based tests** on a regular basis?	
8	Do you have the technology and processes in place to conduct **compatibility testing** on a regular basis?	
9	Do you have the technology and processes in place to conduct **performance testing** on a regular basis?	
10	Do you have the technology and processes in place to conduct **end-to-end testing and penetration testing** on a regular basis?	
11	Are your core security teams ready to **perform vulnerability assessments** before any deployment or redeployment of new or existing applications and infrastructure components?	
12	Have you **established a sound network and infrastructure management structure** using appropriate techniques, methods and protocols that may include implementing automated mechanisms to isolate affected information assets in the event of cyberattacks?	
13	Do you have in place **mechanisms to promptly detect anomalous activities**, including ICT network performance issues and ICT-related incidents, and to identify potential material single points of failure?	

Curious to learn more about DORA and what it may mean for your organization?

Check out our solution brief for more details and insights.

Contrast Security can help secure your applications, enabling your organization to take a key step toward compliance with DORA Regulation (EU 2022/2554).

Schedule a demo

__Note:__ Please be advised that the information provided here and on related materials is not intended to be legal advice. While we strive to ensure the accuracy and reliability of the information, we cannot guarantee the completeness or currency of it. Laws are subject to change, and we cannot be held liable for any actions taken based on the information provided here. If you need legal advice, please consult with a qualified professional.

Contrast SECURITY

contrastsecurity.com