What do you need to know about DORA?

The European financial sector faces growing threat from cyber attacks.

Europe is uniformly strengthening its cybersecurity through The **Digital Operational Resilience Act (DORA).**

In effect from January 17, 2025.
This is what you need to know.

SANS

Why DORA?

Strengthen operational resilience.

Protect consumers and their trust in financial services.

Maintain financial stability across the EU.

Key components

ICT Risk Management:

Comprehensive risk frameworks aligned with business objectives.

Digital Operational Resilience Testing:

Annual vulnerability scans and periodic threatled penetration testing (e.g.,TIBER-EU).

Incident Reporting:

Mandatory reporting of critical incidents within 4 hours.

Information Sharing:

Share cyber threat intelligence within trusted networks.

Third-Party Risk Management:

Oversight and accountability for all critical service providers.

What should you do?

- Conduct gap analysis against DORA requirements.
- Establish governance frameworks with board-level oversight.
- Monitor and manage third-party risks proactively.
- Simulate real-world attacks to test resilience.
- Create a clear response plan for incidents. (which is regularly evaluated)
- Develop detailed documentation of ICT assets and dependencies for regulatory audits.
- Upskill teams in cybersecurity best practices.
- Foster a culture of transparency and continuous improvement.

How SANS can help

Skill and risk assessment

Assess your organization's understanding of how to prevent attacks.

Training and certification

Develop and validate the required capability's needed to comply to DORA.

Scenario based exercises

Execute exercises tailored to your industry and/or situation to help you prepare for DORA.

SANS.org/DORA

What do you need to know about DORA?

SANS

The European financial sector faces growing threat from cyber attacks.
Europe is uniformly strengthening its cybersecurity through The **Digital Operational Resilience Act (DORA).**

In effect from January 17, 2025.
This is what you need to know.

Why DORA?

Strengthen operational resilience.

Protect consumers and their trust in financial services.

Maintain financial stability across the EU.

Key components

ICT Risk Management:

Comprehensive risk frameworks aligned with business objectives.

Digital Operational Resilience Testing:

Annual vulnerability scans and periodic threat-led penetration testing (e.g., TIBER-EU).

Third-Party Risk Management:

Oversight and accountability for all critical service providers.

Incident Reporting:

Mandatory reporting of critical incidents within 4 hours.

Information Sharing:

Share cyber threat intelligence within trusted networks.

What should you do?

- Conduct gap analysis against DORA requirements.
- Establish governance frameworks with board-level oversight.
- Monitor and manage third-party risks proactively.
- Simulate real-world attacks to test resilience.
- Create a clear response plan for incidents. (which is regularly evaluated)
- Develop detailed documentation of ICT assets and dependencies for regulatory audits.
- Upskill teams in cybersecurity best practices.
- Foster a culture of transparency and continuous improvement.

How SANS can help

Skill and risk assessment

Assess your organization's understanding of how to prevent attacks.

Training and certification

Develop and validate the required capability's needed to comply to DORA.

Scenario based exercises

Execute exercises tailored to your industry and/or situation to help you prepare for DORA.

SANS.org/DORA