



# DORA Compliance Checklist

Ensure Your Financial Institution  
is Prepared by January 17, 2025

---

The **Digital Operational Resilience Act (DORA)** is a regulation introduced by the European Union to enhance the **cybersecurity** and **operational resilience** of the financial services industry. With the increasing complexity of cyber threats targeting financial institutions and the growing reliance on third-party service providers, DORA sets out strict requirements to ensure that organizations can withstand, respond to, and recover from ICT (Information and Communication Technology) -related disruptions.

**STEP 1:**

## Understand DORA's Core Requirements

**☐ Identify key areas of compliance**

DORA mandates that financial institutions address the following five core areas:

- ICT Risk Management
- Incident Reporting
- Digital Operational Resilience Testing
- Third-Party Risk Management
- Information Sharing

**☐ Review DORA's specific guidelines**

Ensure that your organization understands both the technical and operational requirements for each core area.

---

**STEP 2:**

## Implement Continuous Testing

**☐ Perform ongoing, real-world cyberattack simulations**

Adopt threat-led penetration testing (TLPT) and adversary emulation to simulate real-world adversary tactics, techniques, and procedures (TTPs). These simulations help continuously assess your organization's ICT systems against evolving threats.

**☐ Expand testing across the ICT infrastructure**

Ensure that breach and attack simulations (BAS) cover all systems, including internal operations and third-party integrations, to detect any vulnerabilities across your entire network.

**☐ Regularly update testing scenarios**

Incorporate the latest threat intelligence into your testing scenarios to ensure your organization remains resilient against new and emerging cyber threats.

**STEP 3:**

## Strengthen Incident Reporting Protocols

 **Create an incident response plan**

Clearly define roles, responsibilities, and procedures for incident detection, response, and reporting.

 **Implement real-time logging tools**

Use automated systems to track ICT-related incidents in real time, ensuring compliance with DORA's 72-hour reporting window.

 **Train teams on reporting procedures**

Regularly conduct training to ensure that staff can efficiently handle incidents and follow the correct reporting protocols.

---

**STEP 4:**

## Enhance Third-Party Risk Management

 **Conduct due diligence on ICT providers**

Assess the security posture of all third-party ICT providers to ensure they meet DORA's stringent security standards.

 **Monitor third-party compliance continuously**

Establish systems to regularly review third-party security defenses, ensuring they remain compliant over time.

 **Maintain a third-party risk register**

Track the compliance status of all third-party providers, and update this information periodically to ensure risks are managed effectively.

**STEP 5:**

## Prepare for Regulatory Reviews

### ❑ Implement a centralized reporting system

Consolidate data from resilience tests, incident reports, and third-party assessments into a single reporting platform.

### ❑ Regularly update internal stakeholders

Ensure that your leadership and compliance teams are consistently informed of your institution's DORA compliance status.

### ❑ Prepare comprehensive documentation

Keep detailed records of your compliance efforts to provide evidence during regulatory reviews or audits.



## Ready to Achieve DORA Compliance?

As the deadline approaches, ensure your financial institution is fully prepared for DORA. Take control of your compliance journey with continuous security testing, adversary emulation, and risk management.

[Try it for yourself with AttackIQ Flex](#) or [request a demo](#) to explore how AttackIQ can help your organization meet DORA's requirements.

#### About AttackIQ

AttackIQ, the leading independent vendor of breach and attack simulation solutions, built the industry's first Breach and Attack Simulation Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework.

The company is committed to supporting its MSSP partners with a flexible Preactive Partner Program that provides turn-key solutions that empower them to elevate client security. AttackIQ is passionate about giving back to the cybersecurity community through its free award-winning AttackIQ Academy and partnership with MITRE Engenuity's Center for Threat-Informed Defense.

For more information visit [www.attackiq.com](http://www.attackiq.com). Follow AttackIQ on [Twitter](#), [LinkedIn](#), and [YouTube](#).