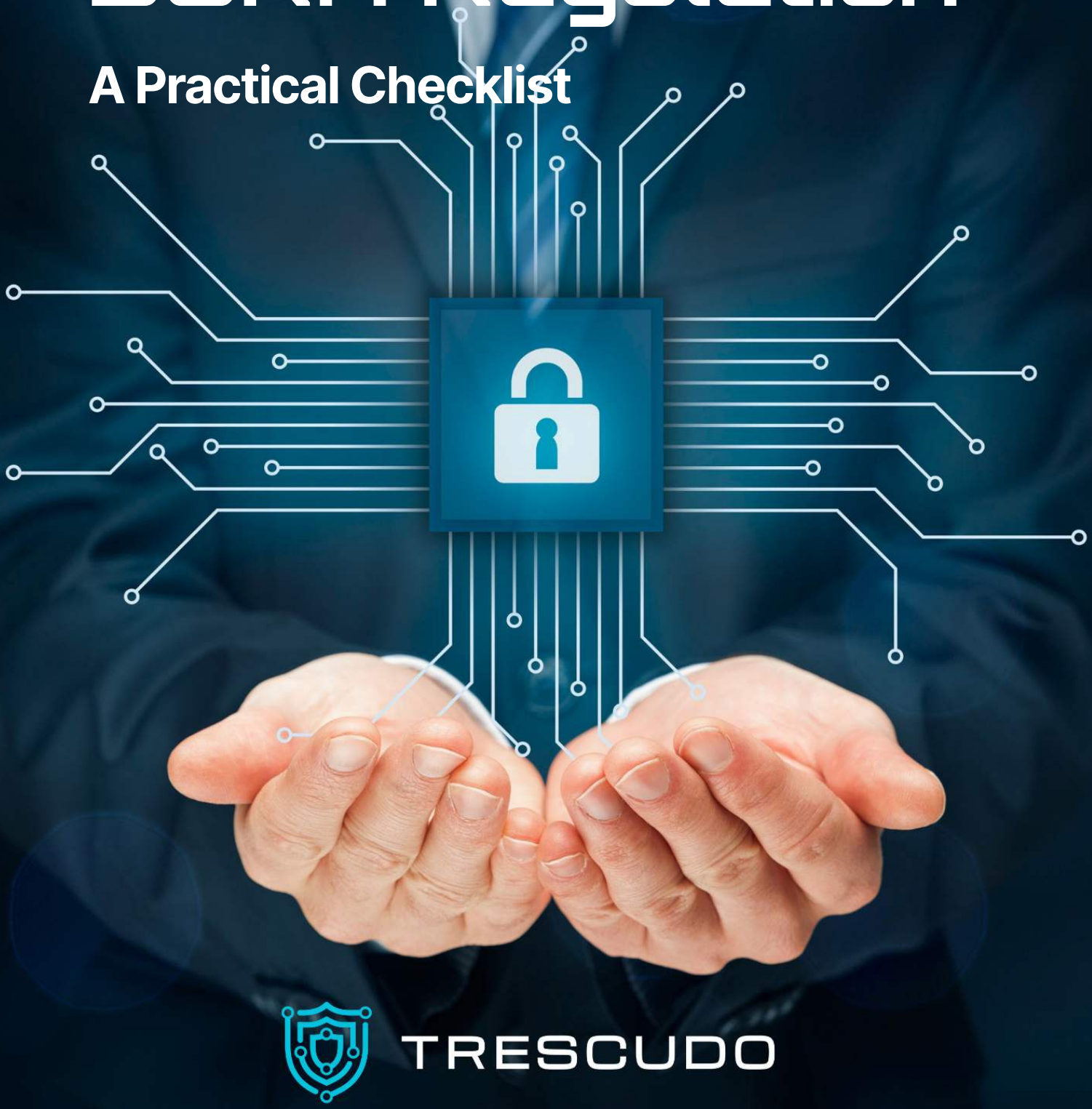
Guide to the DORA Regulation

A Practical Checklist



TRESCUDO

The Trescudo Guide to the DORA Regulation

A Practical Checklist

The EU's Digital Operational Resilience Act (DORA) is a landmark regulation designed to harmonize and strengthen the digital resilience of the financial sector. The deadline for compliance was January 17, 2025. DORA is now in full effect, establishing a binding, comprehensive framework for how financial entities and their critical ICT providers manage digital risks.

At Trescudo, we help businesses navigate complex landscapes. This guide is designed to help you understand your obligations under DORA and assess your readiness against its core pillars.

a) Who Does DORA Apply To?

DORA has a specific scope, targeting the EU's financial ecosystem. It applies to a wide range of financial entities and, crucially, their ICT service providers.

- **Financial Entities:** This includes traditional institutions like banks, insurance companies, and investment firms, as well as newer entities like crypto-asset service providers and crowdfunding platforms.
- **Critical ICT Third-Party Providers:** For the first time, DORA brings critical ICT providers—such as **cloud service providers, data centers, and software providers** that service the financial sector—under direct regulatory oversight.

Note: *For financial entities, DORA acts as "lex specialis," meaning its specific rules for digital operational resilience take precedence over the more general requirements of NIS2.*

DORA is structured around five core pillars that create a comprehensive lifecycle for managing digital risk.

b) The Core Pillars of DORA:

A Readiness Checklist

1. ICT Risk Management

DORA requires a comprehensive and well-documented ICT risk management framework, overseen by the management body.

- [ ] **Governance:** Is your management body actively involved in setting, approving, and overseeing your digital resilience strategy?
- [ ] **Framework:** Have you established and documented a sound, comprehensive ICT risk management framework that identifies, protects, detects, responds to, and recovers from ICT-related incidents?
- [ ] **Asset Management:** Do you maintain a complete and updated inventory of your ICT assets and the information they support?

Entities must have processes to monitor, manage, and report ICT-related incidents.

- [ ] **Incident Classification:** Do you have a process to classify incidents based on criteria defined by the regulation?
- [ ] **Incident Response Plan:** Is there a formal incident response plan in place that ensures a swift and effective response to minimize impact?
- [ ] **Reporting Process:** Have you established a process to report major ICT-related incidents to the relevant competent authorities within the timelines specified by DORA?

2. ICT-Related Incident Management & Reporting

- [ ] **Annual Testing:** Do you conduct annual testing of your critical ICT systems and applications?
- [ ] **Vulnerability Assessments:** Are regular vulnerability scans and assessments part of your testing program?
- [ ] **Threat-Led Penetration Testing (TLPT):** For designated critical entities, are you prepared to conduct in-depth, intelligence-based penetration tests every three years?

3. Digital Operational Resilience Testing

Your defenses must be tested. DORA mandates a proportional and risk-based testing program.

4. Managing ICT Third-Party Risk

You are responsible for the risk introduced by your vendors. DORA places a strong emphasis on supply chain security.

- [ ] **Vendor Strategy:** Do you have a strategy on ICT third-party risk, including a policy on the use of cloud service providers?
- [ ] **Contractual Arrangements:** Do your contracts with ICT providers include specific clauses covering security, access, audit rights, and exit strategies?
- [ ] **Risk Assessment:** Do you assess the risk of all ICT third-party relationships, especially for critical or important functions?

5. Information Sharing

DORA encourages entities to exchange cyber threat information and intelligence.

[ ] Have you established arrangements to share and benefit from cyber threat intelligence with trusted communities or partners to enhance your resilience?

Disclaimer

This checklist is intended for informational and self-assessment purposes only and does not constitute legal advice or a formal compliance audit. The requirements of DORA are complex and their application is unique to each organization's specific circumstances. Trescudo assumes no liability for any actions taken or decisions made based on the information provided in this document. For a formal assessment and tailored guidance, please contact our experts.

c) How Trescudo Supports Your DORA Journey

Achieving and maintaining DORA compliance requires a strategic blend of governance, risk management, and robust technical controls. As your cybersecurity navigator, Trescudo translates these legal requirements into a practical and effective security program.

DORA Pillar	How Trescudo's Offerings Help
ICT Risk Management	Our Cybersecurity Advisory and CISO-as-a-Service offerings help you build the required framework, conduct risk assessments, and establish board-level governance.
Incident Management & Reporting	Our EDR/XDR solutions and 24/7 Managed SOC Services provide the advanced detection, visibility, and response capabilities needed to meet DORA's incident handling requirements.
Digital Operational Resilience Testing	Our Offensive Security team conducts expert Penetration Testing and Vulnerability Assessments to test your defenses and satisfy DORA's testing mandates.
Managing ICT Third-Party Risk	Our Risk Assessment services can be extended to your critical suppliers, helping you manage, document, and mitigate supply chain risk.
Information Sharing	Our Threat Intelligence services provide you with curated, actionable intelligence to proactively defend against emerging threats.

Contact Trescudo Today

The Trescudo Guide to the DORA Regulation offers a practical checklist for financial entities to navigate the complexities of the EU's Digital Operational Resilience Act. Covering essential pillars such as governance, incident management, and third-party risk, this guide equips organizations to enhance their digital resilience in an evolving regulatory landscape. With expert insights and actionable strategies, Trescudo empowers businesses to achieve and maintain compliance while safeguarding their operations against digital threats.

Contact Trescudo today for a strategy session on building and maintaining your digital operational resilience.

TRESCUDO