MITRATECH

DORA Compliance Checklist: Navigating the Digital Operational Resilience Act

A Comprehensive Checklist for Mastering DORA Compliance

EMPOWER. AUTOMATE. ELEVATE.

The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554 is designed to enhance the operational resilience of the financial sector in the European Union. Prior to the implementation of DORA, financial institutions primarily addressed key operational risk categories through capital allocation, overlooking certain components crucial to operational resilience. Post-DORA, they are mandated to adhere to regulations encompassing protection, detection, containment, recovery, and repair capabilities measures specifically targeted at ICT-related incidents. DORA is crucial for companies to ensure they are handling data responsibly and ethically.

Now that you have an understanding of "DORA regulatory framework," it is important to ensure your organization is equipped to take on the compliance requirements.

Consider the following checklist for the 5 domains of the regulation.

1. ICT Risk Management and Governance

Government Framework:

- [ ] Establish and maintain a robust ICT governance framework that includes:
  - [ ] Digital Resilience Strategy
  - [ ] Defined Risk Tolerance (ICT Risk)
  - [ ] Identification, Classification, Documentation of all ICT-Related Business Functions & Information Assets
  - [ ] ICT Policy / Procedure In Line with ESA + ENISA Tech Specs
- [ ] Define roles and responsibilities for ICT risk management

Risk Assessment and Mitigation:

- [ ] Regularly assess and identify ICT risks
- [ ] Develop and implement mitigation strategies for identified risks

Policy Development:

- [ ] Create and maintain comprehensive ICT security policies
- [ ] Ensure policies align with DORA compliance requirements

Security Awareness Training:

- [ ] Provide regular training for employees on ICT security best practices
- [ ] Monitor and measure the effectiveness of training programs. (You can have your employees certified through the DORA website on DORA compliance and the importance of operational resilience!)

2. Incident Response and Reporting

Incident Response Plan:

- [ ] Establish a clear and efficient process for identifying, reporting, and responding to incidents
- [ ] Ensure employees are aware of and understand the reporting procedures

Incident Classification:

- [ ] Clearly define criteria for each incident classification
- [ ] Have a streamlined process to log/classify all ICT incidents and determine major issues
- [ ] Report major incidents through harmonized standard templates

Communication Protocols:

- [ ] Define communication channels and protocols during incidents
- [ ] Establish roles and responsibilities for communication within and outside the organization

Post-Incident Analysis:

- [ ] Conduct thorough post-incident analyses to identify root causes
- [ ] Implement corrective actions based on post-incident findings

Incident Reporting to Authorities:

- [ ] Comply with regulatory requirements for reporting incidents to relevant authorities
- [ ] Maintain documentation of all incident reports and responses

3. Digital Operational Resilience Testing

Testing Framework:

- [ ] Perform periodic basic ICT testing of tools/ systems and advanced Threat Led Penetration Testing (TLPT) for ICT services which impact critical functions
  - [ ] The Threat Led Penetration Testing (TLPT) should be conducted by an external independent tester, scenarios should be approved by regulators and all critical TPPs should be included in TLPT
- [ ] Include scenarios that simulate various cyber threats and disruptions to protect against cyber threats and unauthorized access

Frequency of Testing:

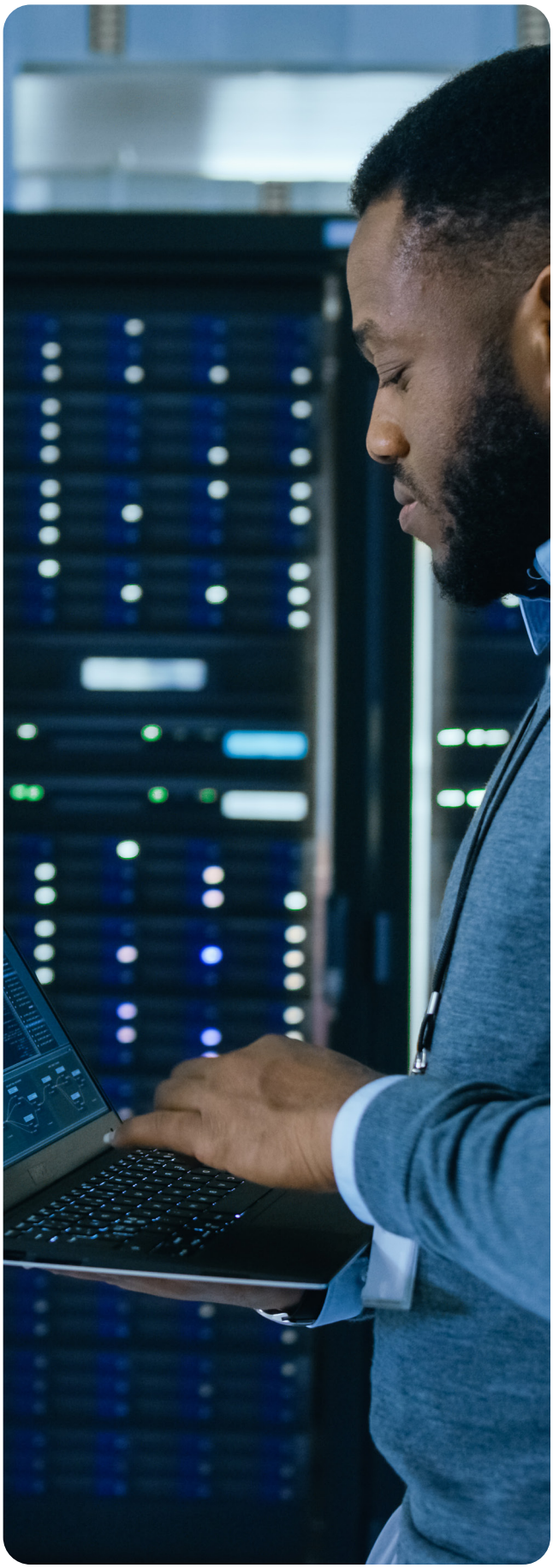
- [ ] Conduct regular risk assessments to identify and evaluate potential threats to the digital operational resilience of your organization
- [ ] Adjust testing frequency based on organizational changes or emerging threats

Documentation:

- [ ] Maintain detailed documentation of digital resilience tests
- [ ] Document lessons learned and improvements identified during testing

Continuous Improvement:

- [ ] Establish a process for continuous improvement based on testing outcomes
- [ ] Regularly update and enhance digital operational resilience strategies



4. Third-Party Risk Management

Vendor Assessment:

- ☐ Implement a comprehensive process for assessing third-party vendors' security measures
- ☐ Ensure vendors meet DORA compliance requirements
- ☐ Assess and manage the operational resilience of third-party service providers

Contractual Obligations:

- ☐ Include specific security and compliance obligations in contracts with third-party vendors
- ☐ Regularly review and update contracts to align with evolving risks

Monitoring and Auditing:

- ☐ Establish ongoing monitoring mechanisms for third-party vendors
- ☐ Conduct periodic audits to ensure compliance with contractual obligations

Incident Response Coordination:

- ☐ Define procedures for coordinating incident responses with third-party vendors
- ☐ Ensure vendors have effective incident response plans in place

Regulatory Alignment:

- ☐ Stay informed about changes in relevant regulations affecting third-party risk management
- ☐ Adjust processes and assessments to meet evolving regulatory requirements

5. Information & Intelligence Sharing Arrangements

Establishment of Arrangements:

- [ ] Collaborate with other financial services institutions to establish information and intelligence sharing arrangements
- [ ] Define the scope, objectives, and governance structure of the sharing arrangements
- [ ] Adapt sharing arrangements to address evolving cyber threats and industry needs

Data Sharing Protocols:

- [ ] Develop protocols for sharing cyber threat intelligence, detection techniques, mitigation strategies, and response procedures
- [ ] Ensure the protocols adhere to privacy and confidentiality requirements as well as relevant regulatory requirements

Threat Intelligence Sharing:

- [ ] Regularly share threat intelligence related to cyber threats affecting the financial services sector
- [ ] Coordinate efforts to identify emerging threats and vulnerabilities

Automating Your DORA Compliance

This checklist is a foundational starting point, emphasizing ongoing adaptation and commitment to continuous improvement for DORA compliance. Familiarize yourself with the key provisions and requirements outlined in DORA and be sure to stay updated on any amendments or additional guidelines.

With DORA preparing to come into full force, you're going to need to have a robust framework – and evidence of that framework – in place for driving operational resilience amidst disruptions. Mitratech's Alyne GRC solution offers a fully centralized and customizable platform for managing compliance with DORA and all other relevant standards, laws, and regulations that impact your organization.

Reach out to our team for more information on how to leverage Mitratech's solutions with the DORA Framework and Regulatory Technical Standards (RTS) already configured. We'll help you accelerate your DORA compliance journey and utilize the powerful advantages of partnering with next-generation GRC technology.

ABOUT MITRATECH

Mitratech is a proven global technology partner for corporate legal, risk, compliance, and HR professionals seeking to maximize productivity, control expense, and mitigate risk by deepening operational alignment, increasing visibility, and spurring collaboration across an enterprise.

Mitratech serves over 14,000 organizations worldwide, spanning more than 160 countries.

For more info, visit: www.mitratech.com

MITRATECH
Syntrio

info@mitratech.com
www.mitratech.com