HOUSE OF CONTROL

Checklist for DORA compliance

This is what you need to establish and follow up

DORA stands for the **Digital Operational Resilience Act**, an EU regulation that comes into effect in January 2025. The goal of the regulation is to make the various IT systems used within the financial sector more robust.

How to comply with this new EU act? That is what we set out to answer in this practical guide. Compliance is an important task, as the financial sector is increasingly dependent on both in-house and outsourced technology to deliver its services.

The intended audience of this guide is ICT professionals and other people helping financial companies comply with DORA. We have added the relevant DORA articles in brackets for each of the following 14+1 steps. For each step we explain in plain language what you need to do to “check the box”.

Disclaimer: *At House of Control, we help our clients navigate DORA requirements regarding third-party ICT risks. Our effective and practical solution is a digital register for all third-party ICT service providers, as mandated by DORA Article 28 (3). It has been developed together with one of the largest finance institutions in the Nordics to help our clients in its work with complying with the DORA requirements.*

House of Control is a software company. We do not offer DORA compliance consulting services. Thus, ***following the checklist does not guarantee compliance with all DORA legal requirements****. The contents of the checklist are based on our own research of the DORA requirements, and includes inspiration from various actors offering compliance services. We do not assume any responsibility or liability for any failure to comply with DORA requirements or resulting from the use of the checklist.*

- [ ] **1. A governance and control framework for the management of ICT risks *(Article 5)***
  Create a formal reporting process where the board or management body receives regular updates on ICT risks, incidents, and resilience strategies. Ensure this is part of a quarterly review cycle, with the ability to escalate reports for significant incidents. Include a clear process for board approval and oversight of the overall digital operational resilience strategy.

- [ ] **2. ICT risk reporting and governance at board level *(Article 5)***
  Create a formal reporting process where the board or management body receives regular updates on ICT risks, incidents, and resilience strategies. Ensure this is part of a quarterly review cycle, with the ability to escalate reports for significant incidents. Include a clear process for board approval and oversight of the overall digital operational resilience strategy.

- [ ] **3. Internal audit and assessment program for ICT systems and digital resilience *(Article 5)***
  Establish an internal audit program that conducts periodic reviews of your ICT governance, risk management, and incident response capabilities. Document all findings and ensure there is a defined follow-up process for addressing any gaps or deficiencies, reporting them back to senior management.

- [ ] **4. A framework for ICT risk management as part of your company-wide risk management system (Article 6)**
  Integrate ICT risk management into your company's broader risk management framework. Document your risk analysis methodology and maintain a risk register with action plans and scheduled assessments. The framework should also categorize risks by priority and clearly define the organization's risk appetite and tolerance, accounting for evolving threats like ransomware.

- [ ] **5. An inventory with all information assets and ICT assets *(Article 8)***
  Maintain a digital inventory of all ICT and information assets. Ensure this is regularly updated to reflect changes, including asset classifications based on criticality and sensitivity. Your inventory must track data flows between ICT systems and third-party providers, and you should continuously monitor these connections.

- [ ] **6. An ICT security policy *(Article 9)***
  Develop and enforce an ICT security policy that outlines protective measures for system availability, integrity, and security. This should include user access control, change management, encryption, and patching processes. Establish procedures for managing user access (e.g., least privilege, MFA), and implement monitoring mechanisms to detect unauthorized access or other anomalies. Ensure incident response processes are included.

- [ ] **7. An ICT business continuity plan *(Articles 11-12)***
  Build a business continuity plan (BCP) that includes a business impact analysis, communication strategies, and periodic testing. Test scenarios should replicate realistic disruptions, including third-party ICT failures. Ensure test results are documented and any gaps are addressed and reported to senior management. The BCP should also include redundancy strategies for third-party failures and communication protocols with stakeholders, such as regulators.

- [ ] **8. Procedures for data back-up and recovery *(Article 12)***
  Create a formal reporting process where the board or management body receives regular updates on ICT risks, incidents, and resilience strategies. Ensure this is part of a quarterly review cycle, with the ability to escalate reports for significant incidents. Include a clear process for board approval and oversight of the overall digital operational resilience strategy.

- [ ] **9. Training programs for ICT security awareness *(Article 13)***
  Establish and maintain ICT security awareness and resilience training programs. These should be compulsory for all staff and include practical exercises like phishing simulations. Management-level staff should also receive specialized training focused on managing ICT risks, regulatory reporting, and incident handling.

- [ ] **10. An ICT-related incident management process *(Article 17-23)***
  Design a process for detecting and managing ICT-related incidents. This should include maintaining an incident register and using standardized templates for reporting. Ensure the process includes root cause analysis, escalation procedures to senior management, and compliance with regulatory timelines for reporting incidents.

- [ ] **11. Framework for ICT incident reporting to competent authorities *(Article 18-23)***
  Develop clear protocols for reporting major ICT incidents to relevant authorities. Ensure that reporting complies with regulatory timelines and formats. Define what constitutes a "major incident" and establish a system for continuous monitoring and follow-up reporting to authorities.

- [ ] **12. A risk-based digital operational resilience testing program *(Article 24-27)***
  Develop a comprehensive testing program that includes advanced threat simulations, such as penetration testing and red teaming. The results of these tests should feed back into your risk management assessments and include disaster scenario stress tests.

13.An outsourcing risk management policy
(Article 28)

- [ ] Implement an outsourcing policy that requires thorough risk assessments of third-party ICT service providers. Ensure due diligence before entering agreements, and define risk thresholds and performance metrics. Establish continuous monitoring and regular reassessment of third-party risks, especially for cloud services.

14. Policies for the use of third-party ICT service providers supporting critical functions
(Articles 28-30)

- [ ] Maintain a register of all third-party ICT service providers, with a focus on critical functions. Ensure contracts include key terms and conditions for service levels and exit strategies. Regularly test exit strategies to ensure data portability and smooth transitions, without disrupting business operations.

House of Control offers a digital register to manage the requirements of Article 28: “As part of their ICT risk management framework, financial entities shall maintain and update at entity level, and at sub-consolidated and consolidated levels, a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers.”

14. ICT risk insurance strategy
(optional but recommended)

- [ ] Consider purchasing an ICT risk insurance policy to cover potential financial losses from cyberattacks, data breaches, system outages, or third-party failures. This should supplement other risk mitigation strategies and provide a financial safeguard against extreme events.