Operational Due Diligence & DORA

Document updated on 20/01/2025

1. Governance and Responsibilities

a. Establishment of DORA Governance

- What roles and responsibilities have been defined within your organisation to ensure DORA compliance?
- Who is the designated lead for digital business resilience?
- Can you provide evidence of board and senior management training or awareness of DORA requirements?

b. Digital Risk Management Policy

- Have you developed a documented ICT (Information and Communications Technology) risk management policy that complies with DORA?
- How often is this policy updated?
- Can you provide an example or extract of this policy?

---

2. Identifying and managing ICT risks

a. Digital Risk Assessment

- What processes are in place to identify, assess and document ICT-related risks?
- Do you have an ICT risk map? Can you share it?

b. Outsourcing and third parties

- Who are your main external suppliers of ICT services?
- How do you assess the risks associated with outsourcing critical functions (including information systems management)?
- Can you provide due diligence or assessment reports on critical ICT providers?

c. **ICT Incident Management**

- Do you have an ICT incident management process in place?
- Can you provide an example of a recent incident report and the corrective actions taken?
- How often do you test and simulate ICT incidents?

---

3. Business Continuity and Resilience Plan

a. **Business Continuity Plan (BCP)**

- Do you have a specific BCP for ICT systems?
- When was the BCP last tested? What were the results of the test?
- Can you provide copies of the BCP and associated test reports?

b. **Disaster Recovery Plan (DRP)**

- Do you have a DRP for your critical digital infrastructure and data?
- Can you describe the principles for backing up company data (frequency, redundancy, infrastructure used)?
- Can you provide the documentation and results of the most recent DRP tests?
- Did these tests identify any gaps or areas for improvement?

---

4. **Monitoring and reporting**

a. Continuous monitoring of ICT risks

- What tools or processes do you use to monitor critical ICT systems in real time?
- How are alerts and incidents escalated within the organisation?

b. Regulatory reporting

- Do you have a process for reporting major ICT incidents to the relevant authorities?
- Can you provide an example (anonymised if necessary) of an incident report submitted to an authority?

c. Dashboards and monitoring indicators

- What KPIs or dashboards do you use to monitor ICT compliance and resilience?
- How are these indicators communicated to senior management and the board?

---

5. Management of third parties and subcontractors

a. Contracts and clauses related to DORA

- Do your contracts with third parties contain specific clauses relating to DORA compliance?
- Can you provide an example of a contract with such clauses?

b. Third party audits

- How often do you audit your critical service providers?
- Can you provide reports or certificates of the most recent audits?
- Can you tell us if the service providers you use to implement and monitor your ICT and data security are certified (PASSI, SecNumCloud, ISO 27001, etc.)?

c. Third party resilience plans

- Have your ICT providers shared their digital operational resilience plans?
- How do you validate their ability to meet regulatory requirements, including DORA?

---

6. Tests and simulations

a. Penetration testing and cyber security

- How often do you perform penetration tests on your ICT systems?
- Can you provide recent reports or results of these tests?

b. Crisis exercises

- Have you recently conducted crisis or cyber attack simulation exercises?
- What were the lessons learned and actions taken following these exercises?

---

7. Documentation and evidence

a. Archiving and Access to Evidence

- How do you ensure that documents relating to DORA compliance are archived and traceable?
- Can you provide a sample of archived documents relating to your ICT policies or incident reports?

b. Internal Control and Internal Auditing

- Does your internal audit department conduct specific reviews of DORA compliance?
- Can you provide reports from recent internal audits?

8. Awareness-raising and training

a. Employee training

- What awareness and training programs have you put in place for your employees on DORA requirements?
- Can you provide evidence of training (schedule, materials, certificate)?

b. Third party training

- Do you require your service providers or partners to undergo specific training to comply with DORA?