CHECKLIST

DORA Compliance

This checklist is designed to help your organisation achieve compliance with the Digital Operational Resilience Act (DORA). It covers essential areas and tasks to prepare your infrastructure and operations for regulatory demands.

Adapt this checklist according to your organisation's size, structure, and risk exposure.

Instructions:

- Review each section and its corresponding tasks thoroughly.
- Use the checkbox to mark each task upon completion.
- Utilise the "Notes" section to document any critical insights or specific conditions encountered during the task execution.

DORA Focus Areas

1. ICT Risk Management

- [ ] **Inventory:** Confirm the existence of a detailed inventory covering all ICT components including hardware, software, networks, and cloud services.
- [ ] **Risk Assessments:** Ensure risk assessments are periodically conducted to identify, analyse, and prioritise system vulnerabilities and threats.
- [ ] **Risk Controls:** Implement and maintain robust controls like firewalls, access controls, and encryption to safeguard against ICT risks.
- [ ] **Incident Reporting:** Establish and disseminate clear procedures for reporting ICT-related incidents.
- [ ] **Disaster Recovery:** Maintain an up-to-date and tested disaster recovery plan that aligns with organisational resilience goals.

Notes:

2. Incident Management

- [ ] **Classification Criteria:** Define and standardise criteria for the classification of ICT incidents based on their severity and impact.
- [ ] **Communication Protocols:** Set up formal communication protocols to ensure timely escalation and reporting of ICT incidents.
- [ ] **Incident Response Procedures:** Document and regularly update procedures for the effective management of ICT incidents.
- [ ] **Incident Response Testing:** Regularly schedule incident response drills to test and improve team readiness and procedural efficacy.

Notes:

3. Reporting

- [ ] **Reporting Requirements:** Clearly understand and document the reporting obligations under DORA, including the types of incidents that must be reported and the authorities involved.
- [ ] **Reporting Processes:** Develop and implement efficient processes for the timely and accurate reporting of incidents and breaches to meet regulatory timelines.

Notes:

4. Governance and Oversight

- [ ] **Roles and Responsibilities:** Clearly delineate and communicate the roles and responsibilities associated with DORA compliance within your organisation.
- [ ] **DORA Compliance Program:** Ensure there is a dedicated program for DORA compliance, complete with allocated resources and authority.
- [ ] **Risk Management Integration:** Seamlessly integrate DORA compliance requirements into your existing risk management frameworks to enhance governance.
- [ ] **Compliance Reviews:** Regularly perform comprehensive reviews and updates to the DORA compliance program to adapt to evolving regulations and organisational changes.

Notes:

5. Third-Party Risk Management

- [ ] **Third-Party Identification:** Compile and regularly update a list of all third-party ICT service providers upon whom your organisation relies.
- [ ] **Third-Party Risk Assessments:** Regularly conduct detailed risk assessments to evaluate the security measures and compliance posture of third-party vendors.
- [ ] **Contractual Safeguards:** Ensure that contracts with third-party vendors include clauses mandating compliance with DORA.
- [ ] **Third-Party Monitoring:** Implement ongoing monitoring strategies to detect and manage risks associated with third-party ICT service providers.

Notes:

This checklist serves as a foundational tool to guide your organisation toward DORA compliance. Regularly revisiting and updating this checklist will ensure that your compliance efforts are effective and up-to-date.

Date: