CybelAngel

Recommendations for implementing DORA

In order to meet and maintain compliance, focus on the following 5 areas.

Follow an ICT risk management framework

- [ ] Conduct a comprehensive risk assessment to identify vulnerabilities in ICT systems.
- [ ] Map critical ICT assets and their dependencies to business functions.
- [ ] Assign clear roles and responsibilities for managing ICT risks.

Third-Party risk management

- [ ] Vet all critical third-party ICT service providers to ensure they meet DORA standards before entering contracts.
- [ ] Update contracts to include detailed provisions on data security, storage locations, and incident response protocols.
- [ ] Conduct regular audits and ensure third-party providers participate in training programs on cyber resilience.
- [ ] Develop robust exit strategies to mitigate risks when terminating contracts with non-compliant providers.

Implement incident reporting mechanisms

- [ ] Set up standardized templates for reporting major ICT incidents to competent authorities.
- [ ] Notify clients promptly about incidents and outline mitigation measures.
- [ ] Perform root-cause analyses for all incidents to prevent recurrence.

Conduct regular resilience testing

- [ ] Schedule annual threat-led penetration testing (TLPT) to simulate real-world cyberattacks.
- [ ] Use the results of these tests to refine operational resilience strategies.