CLICKSECURE.AI

NIS 2 & DORA Readiness Checklist

A practical self-assessment for essential, important and financial entities.

Work through each item, tick what is already in place, and turn the gaps into a plan. Free to use and share.

NIS 2 readiness

NIS 2 (Directive (EU) 2022/2555) expands scope and raises minimum security measures. Article 21(2) lists the ten baseline measures (a-j); management bodies (Art. 20) are accountable for approving and overseeing them, and incidents must be reported on the Art. 23 timeline.

Governance & accountability (Art. 20)

- ☐ Management body formally approves and oversees the cyber risk-management measures.
- ☐ Management and key staff complete cybersecurity risk training.
- ☐ Roles, responsibilities and an accountable owner for cybersecurity are defined.

(a) Risk analysis & information system security policies

- ☐ Documented risk analysis and information system security policies.
- ☐ Asset inventory and data classification kept up to date.

(b) Incident handling

- ☐ Incident detection, handling and response procedures, tested.

(c) Business continuity & crisis management

- ☐ Backup management, disaster recovery and crisis management, tested regularly.

(d) Supply chain security

- ☐ Security requirements and assessment for direct suppliers and service providers.

(e) Security in acquisition, development & maintenance

- ☐ Secure acquisition, development and maintenance, including vulnerability handling and disclosure.

(f) Effectiveness assessment

- ☐ Policies and procedures to assess the effectiveness of the measures (audits, tests, pentests).

(g) Cyber hygiene & training

- ☐ Basic cyber hygiene practices and cybersecurity awareness training for all staff.

(h) Cryptography & encryption

- ☐ Policies on the use of cryptography and, where appropriate, encryption.

(i) HR security, access control & asset management

- ☐ Human resources security (screening, joiners/movers/leavers, timely access revocation).
- ☐ Access control with least privilege and asset management.

(j) MFA & secured communications

- ☐ Multi-factor or continuous authentication.
- ☐ Secured voice, video and text communications and emergency communication, where appropriate.

Incident reporting timeline (Art. 23)

- ☐ Ability to meet deadlines: 24h early warning, 72h notification, final report within one month.

DORA readiness

DORA (Regulation (EU) 2022/2554) sets digital operational resilience rules for financial entities and their ICT providers, built on five pillars.

Pillar 1 - ICT risk management

- ☐ Board-approved ICT risk-management framework, reviewed regularly.
- ☐ Mapping of ICT assets, business functions and dependencies.
- ☐ ICT business continuity policy, response and recovery plans, and tested backups.

Pillar 2 - ICT-related incident management & reporting

- ☐ Detect, classify and report major ICT-related incidents to the competent authority.

Pillar 3 - Digital operational resilience testing

- ☐ Regular resilience testing programme (vulnerability assessments, scenario tests).
- ☐ Threat-Led Penetration Testing (TLPT) for entities in scope.

Pillar 4 - ICT third-party risk management

- ☐ Register of ICT third-party providers, contractual requirements and concentration-risk monitoring.

Pillar 5 - Information sharing

- ☐ Arrangements to share cyber threat intelligence with peers.

This checklist is a practical guide, not legal advice. Specific obligations depend on your sector, size and role under each framework. Sources: Directive (EU) 2022/2555 (NIS 2), Art. 20, 21 & 23; Regulation (EU) 2022/2554 (DORA).