




DORA compliance checklist

Digital Operational Resilience Act (EU Regulation 2022/2554)

How to use this checklist

For each requirement mark Done / N.a. and record evidence (link, ticket ID, document path, date) so auditors can verify. Review quarterly or after any major organisational, technical or regulatory change.

 This guide is for information only and is not legal advice. Confirm applicability with your legal or compliance team.

| | |
|----------------------|-------------------------------------|
| <input type="text"/> | <input checked="" type="checkbox"/> |
| <input type="text"/> | <input checked="" type="checkbox"/> |
| <input type="text"/> | <input checked="" type="checkbox"/> |
| <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="checkbox"/> |
| <input type="text"/> | <input type="checkbox"/> |

1. Governance & organisational oversight

| Requirement | Guidance & evidence ideas | Status |
|--|---|--------------------------|
| 1.1 Corporate registration / Legal certificates | <ul style="list-style-type: none">• Minutes of board meetings; resolution ID.• Strategy document version control showing review dates. | <input type="checkbox"/> |
| 1.2. Senior management receives quarterly DORA-status reports. | <ul style="list-style-type: none">• Reports filed in GRC tool; distribution list. | <input type="checkbox"/> |
| 1.3. Roles and responsibilities for ICT risk and incident response are formally defined. | <ul style="list-style-type: none">• RACI matrix covering board, CISO, CIO, risk, audit. | <input type="checkbox"/> |
| 1.4. Policies for ICT risk, incident handling, BCP/DRP and third-party oversight exist and are reviewed at least annually. | <ul style="list-style-type: none">• Policy index with owners and next-review dates. | <input type="checkbox"/> |
| 1.5. A communication & escalation matrix for ICT incidents is documented and published internally. | <ul style="list-style-type: none">• Flow-chart in IRP; phone tree; emergency contact list. | <input type="checkbox"/> |

2. ICT risk management framework

| Requirement | Guidance & evidence ideas | Status |
|--|--|--------------------------|
| 2.1. Inventory of critical ICT assets is complete and reviewed quarterly. | <ul style="list-style-type: none">• CMDB extracts; asset-criticality tags. | <input type="checkbox"/> |
| 2.2. Standardised risk-assessment methodology is applied (likelihood x impact) and aligned with ISO 27005/ENISA. | <ul style="list-style-type: none">• Methodology document; sample completed assessments. | <input type="checkbox"/> |
| 2.3. Risk-treatment plan identifies mitigating controls, owners and deadlines. | <ul style="list-style-type: none">• Risk register with residual-risk ratings and status. | <input type="checkbox"/> |
| 2.4. Key risk indicators (KRIs) / KPIs trigger alerts when thresholds are breached. | <ul style="list-style-type: none">• Dashboard screenshots; alert-routing rules. | <input type="checkbox"/> |
| 2.5. Annual management review evaluates framework effectiveness and approves improvements. | <ul style="list-style-type: none">• Review report signed by CIO/CRO. | <input type="checkbox"/> |

3. ICT incident management

| Requirement | Guidance & evidence ideas | Status |
|--|--|--------------------------|
| 3.1. 24 x 7 monitoring (SIEM/EDR/NDR) covers all critical systems with tested alerting. | <ul style="list-style-type: none">• Monitoring coverage map; on-call rota. | <input type="checkbox"/> |
| 3.2. Incident response plan (IRP) includes classification criteria, playbooks, decision trees, regulatory timelines. | <ul style="list-style-type: none">• IRP version and distribution proof. | <input type="checkbox"/> |
| 3.3. IRP is tested at least annually (tabletop + live technical exercise). | <ul style="list-style-type: none">• Exercise reports; action items closed. | <input type="checkbox"/> |
| 3.4. Root-cause analysis (RCA) is performed for all major incidents using e.g. 5-Whys, fishbone. | <ul style="list-style-type: none">• RCA template; sample completed RCAs. | <input type="checkbox"/> |
| 3.5. DORA reporting workflow submits initial report within 24 h, update within 72 h, final within 1 month. | <ul style="list-style-type: none">• Ticket workflow; regulator acknowledgements. | <input type="checkbox"/> |

4. Digital operational resilience testing

| Requirement | Guidance & evidence ideas | Status |
|---|---|--------------------------|
| 4.1. Annual vulnerability scans and authenticated penetration tests are performed across all in-scope assets. | <ul style="list-style-type: none">• Scan reports; pen-test statements of work. | <input type="checkbox"/> |
| 4.2. Threat-led penetration testing (TLPT) using TIBER-EU or CBEST methodology is run at least every three years for critical services. | <ul style="list-style-type: none">• Test-scope approval by competent authority. | <input type="checkbox"/> |
| 4.3. Capacity stress and fail-over tests validate RTO/RPO objectives. | <ul style="list-style-type: none">• Test results showing time-to-recover. | <input type="checkbox"/> |
| 4.4. Findings are prioritised (high/medium/low) and tracked to closure; overdue items escalated. | <ul style="list-style-type: none">• Remediation tracker; evidence of fixes. | <input type="checkbox"/> |
| 4.5. Senior management reviews and signs off the annual test schedule and results. | <ul style="list-style-type: none">• Sign-off sheet; presentation deck. | <input type="checkbox"/> |

5. Third-party risk management

| Requirement | Guidance & evidence ideas | Status |
|---|---|--------------------------|
| 5.1. Central register lists all ICT-third-party contracts, data-flows, criticality ratings and cloud regions. | <ul style="list-style-type: none">• TPRM platform export. | <input type="checkbox"/> |
| 5.2. Pre-contract due diligence covers financial, security and regulatory compliance posture. | <ul style="list-style-type: none">• Due-diligence questionnaire; SOC 2 / ISO 27001 reports. | <input type="checkbox"/> |
| 5.3. Contracts embed: security SLAs, right-to-audit, breach notification < 24 h, data-location clauses, exit & portability. | <ul style="list-style-type: none">• Signed contract excerpts. | <input type="checkbox"/> |
| 5.4. Ongoing monitoring includes service reviews, attestation reviews, risk re-assessments at least annually. | <ul style="list-style-type: none">• Vendor scorecards; re-assessment logs. | <input type="checkbox"/> |
| 5.5. Concentration risk (critical services on same provider) and sub-outsourcing chains are analysed and reported. | <ul style="list-style-type: none">• Concentration-risk heat-map; board briefing. | <input type="checkbox"/> |

6. Business continuity & disaster recovery

| Requirement | Guidance & evidence ideas | Status |
|---|--|--------------------------|
| 6.1. Business impact analysis (BIA) defines RTO/RPO and maximum tolerable outage for each critical process. | <ul style="list-style-type: none">• BIA workbook; approval signatures. | <input type="checkbox"/> |
| 6.2. Business continuity plan (BCP) covers cyber, physical, pandemic, supply-chain scenarios. | <ul style="list-style-type: none">• BCP chapters; distribution list. | <input type="checkbox"/> |
| 6.3. Disaster recovery plan (DRP) details technical recovery run-books and fail-over procedures. | <ul style="list-style-type: none">• DRP run-book; automation scripts. | <input type="checkbox"/> |
| 6.4. Off-site and immutable backups are taken at least daily; restore tests performed quarterly. | <ul style="list-style-type: none">• Backup schedules; restore-test logs. | <input type="checkbox"/> |

| Requirement | Guidance & evidence ideas | Status |
|---|---|--------------------------|
| 6.5. Annual BCP/DRP exercises include full data-centre fail-over and crisis-communications drill. | <ul style="list-style-type: none"> • Exercise after-action report; improvement plan. | <input type="checkbox"/> |

7. Information sharing & reporting

| Requirement | Guidance & evidence ideas | Status |
|---|--|--------------------------|
| 7.1. Organisation participates in sectoral information-sharing bodies (e.g. FS-ISAC, ECSC FIN-CERT). | <ul style="list-style-type: none"> • Membership confirmation; mailing-list archive. | <input type="checkbox"/> |
| 7.2. Procedures enable secure, anonymised threat-intelligence sharing (STIX/TAXII) without breaching confidentiality. | <ul style="list-style-type: none"> • Sharing policy; anonymisation workflow. | <input type="checkbox"/> |
| 7.3. Internal rapid-alert channel (e.g. Slack #threat-intel) broadcasts high-severity advisories within two hours. | <ul style="list-style-type: none"> • Channel screenshots; distribution stats. | <input type="checkbox"/> |
| 7.4. Records of all inbound/outbound intelligence are retained for minimum five years in line with DORA. | <ul style="list-style-type: none"> • Log-retention policy; storage location. | <input type="checkbox"/> |

8. Documentation, record-keeping & continuous improvement

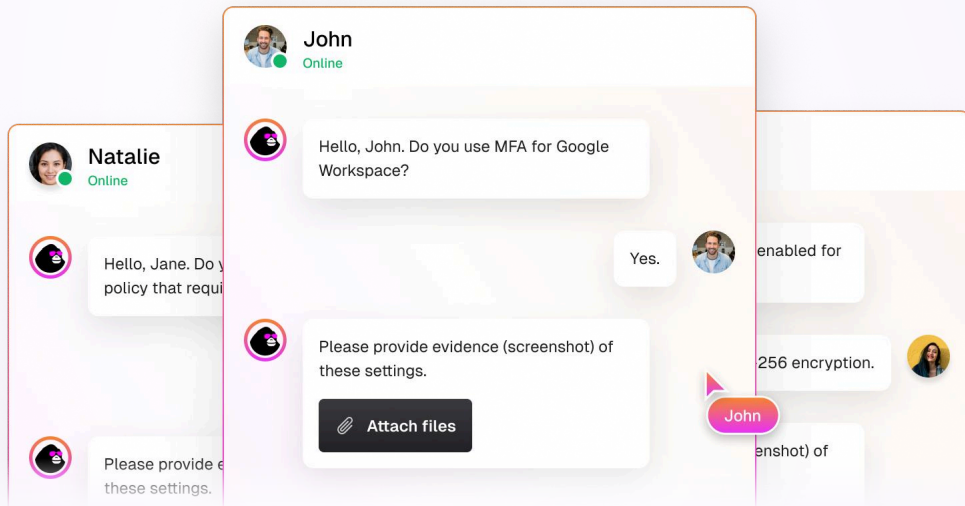
| Requirement | Guidance & evidence ideas | Status |
|---|---|--------------------------|
| 8.1. Centralised repository stores policies, risk assessments, incident logs, test reports and evidence for ≥ five years. | <ul style="list-style-type: none"> • SharePoint / Confluence / GRC repository map. | <input type="checkbox"/> |
| 8.2. Quarterly gap-analysis against DORA, EBA/ESMA/EIOPA guidelines and national transpositions is documented. | <ul style="list-style-type: none"> • Gap-analysis template; management actions. | <input type="checkbox"/> |

| Requirement | Guidance & evidence ideas | Status |
|--|--|--------------------------|
| 8.3. Internal-audit programme covers DORA controls at least once every three years; findings tracked to closure. | • Audit plan; finding tracker. | <input type="checkbox"/> |
| 8.4. Organisation-wide training ensures employees understand DORA obligations and role-specific procedures. | • LMS completion reports; training slides. | <input type="checkbox"/> |
| 8.5. KPIs/KRIs (e.g. MTTR, patch-latency, vendor risk scores) are reviewed quarterly and feed continuous-improvement projects. | • Quarterly risk-committee minutes; improvement backlog. | <input type="checkbox"/> |

Appendix

Quick reference to DORA articles

| Title | Regulation reference |
|--|----------------------|
| ICT-risk management framework | Art. 5–9 |
| Incident reporting | Art. 17–23 |
| Digital operational resilience testing | Art. 24–29 |
| ICT third-party risk | Art. 30–44 |
| Information sharing | Art. 45 |
| Oversight & enforcement | Art. 46–59 |



Tired of endless custom security questionnaires? **Ease the burden with Copla**

The Copla team is deeply knowledgeable about DORA and the complexities of third-party risk management. We simplify these challenges with expertise and real-time support, ensuring your vendor ecosystem remains resilient and compliant.

[Book a demo](#) ▶

More info available on copla.com

Further reading & resources

🌟 Success stories: [Learn how we help our clients](#)

📖 Download [Mastering third-party risk management under DORA](#) eBook

📖 Visit our [blog](#) for more resources