Kodem · Compliance Toolkit

# DORA ICT Risk Self-Assessment Template

Evidence your operational resilience across DORA's five pillars.

The Digital Operational Resilience Act has been in force since 17 January 2025. Article 6 asks financial entities to maintain an ICT risk management framework that continuously identifies risks to operational resilience. Article 8 asks them to identify, classify and document every ICT-supported business function and its dependencies on an ongoing basis.

This template is structured around the same five pillars an auditor will walk through. Use it before your next internal review to capture which ICT risks are material to your critical functions, where the evidence lives, and whether remediation is proportionate. Type into the fields, mark the checkboxes, and note your maturity level.

## How to use this template

- Complete the organisation profile, then work through each of the five pillars.
- For every pillar, record the evidence you can produce today, not the policy that says it should exist.
- Be honest in the maturity fields. The gaps are the point of the exercise.
- Bring the completed template to internal audit before your next external DORA review.

# Organisation profile

Establish who is completing this assessment and the scope it covers.

**Financial entity / institution name**

**Assessment owner (name & role)**

**Assessment date**

**Review period covered**

**Critical or important functions in scope (e.g. payment initiation, KYC, settlement)**

**Lead supervisory authority**

**Next external review date**

## Maturity scale used in this template

| | |
|---|---|
| **Initial** | Ad hoc or undocumented. Evidence would have to be reconstructed. |
| **Developing** | Some evidence exists but is partial or not current. |
| **Defined** | Documented and repeatable. Evidence is available on request. |
| **Managed** | Continuous, current evidence tied to critical functions. |

01

# ICT Risk Management

Articles 5-15

**What the auditor is asking**

Auditors want continuous identification and classification of risk against critical functions, the function-to-finding mapping in real time, not a quarterly export.

**Self-assessment**

| | YES | PARTIAL | NO |
|---|---|---|---|
| Can you produce a current mapping of ICT risks to the critical / important functions they affect? | ☐ | ☐ | ☐ |
| Is risk classification continuous (live) rather than a periodic export? | ☐ | ☐ | ☐ |
| Can you show which scanner findings are reachable in production vs. dormant? | ☐ | ☐ | ☐ |
| Is remediation effort prioritised by materiality to operational resilience? | ☐ | ☐ | ☐ |

Evidence available today (where it lives, format, how current)

Largest gap / action to close it

Maturity

Initial

02

# ICT-Related Incident Reporting

Articles 17-23

**What the auditor is asking**

When a vulnerability becomes an incident, regulators want the blast radius: which services were affected and which customer journeys touched the vulnerable code.

**Self-assessment**

| | YES | PARTIAL | NO |
|---|---|---|---|
| Can you determine the blast radius of an incident without a forensics project? | ☐ | ☐ | ☐ |
| Do you have an audit trail linking a vulnerable component to affected services? | ☐ | ☐ | ☐ |
| Can you map an incident to the specific customer journeys it touched? | ☐ | ☐ | ☐ |
| Are reporting timelines and thresholds documented and tested? | ☐ | ☐ | ☐ |

**Evidence available today (incident trail, reachability data, runbooks)**

**Largest gap / action to close it**

**Maturity**

Initial

03

# Digital Operational Resilience Testing

Articles 24-27 · incl. Threat-Led Penetration Testing

**What the auditor is asking**

Red teams need to scope exercises against critical functions and the components that support them. Evidence tells them, and the regulator, which components actually matter.

**Self-assessment**

| | YES | PARTIAL | NO |
|---|---|---|---|
| Are resilience tests scoped against your critical / important functions? | ☐ | ☐ | ☐ |
| Can you identify which components actually support each critical function? | ☐ | ☐ | ☐ |
| Is TLPT scoping informed by what runs in production rather than the full estate? | ☐ | ☐ | ☐ |
| Are test findings tracked back to the functions and components they affect? | ☐ | ☐ | ☐ |

Evidence available today (test scope docs, component inventory)

Largest gap / action to close it

Maturity

Initial

04

# ICT Third-Party Risk

Articles 28-44

### What the auditor is asking

Most third-party exposure lives in open-source dependencies vendors ship inside their software. Knowing which dependencies execute turns an unmanageable SBOM into a short list worth scrutinising.

**Self-assessment**

| | YES | PARTIAL | NO |
|---|---|---|---|
| Do you maintain an SBOM / register of third-party and open-source dependencies? | ☐ | ☐ | ☐ |
| Can you show which of those dependencies actually execute in your environment? | ☐ | ☐ | ☐ |
| Are dormant (imported-but-unused) components distinguished from active ones? | ☐ | ☐ | ☐ |
| Is third-party scrutiny prioritised by what is reachable, not just what is present? | ☐ | ☐ | ☐ |

Evidence available today (SBOM, dependency reachability, contracts)

Largest gap / action to close it

Maturity

Initial

05

# Information Sharing

Article 45



**What the auditor is asking**

When the sector circulates intelligence on a newly weaponised CVE, you should be able to tell within minutes whether it is reachable in your production estate, turning a sector-wide alert into a specific decision.

**Self-assessment**

| | YES | PARTIAL | NO |
|---|---|---|---|
| Do you participate in sector threat-intelligence sharing arrangements? | ☐ | ☐ | ☐ |
| Can you assess reachability of a newly disclosed CVE within minutes? | ☐ | ☐ | ☐ |
| Is there a defined path from a sector alert to a prioritised internal decision? | ☐ | ☐ | ☐ |
| Are sharing arrangements documented and reviewed? | ☐ | ☐ | ☐ |

Evidence available today (intel feeds, reachability response process)

Largest gap / action to close it

Maturity

Initial

# Summary & sign-off

Consolidate the picture and record who owns the next steps.

| PILLAR | MATURITY | PRIORITY ACTION |
|---|---|---|
| ICT Risk Management | Initial | |
| ICT-Related Incident Reporting | Initial | |
| Operational Resilience Testing | Initial | |
| ICT Third-Party Risk | Initial | |
| Information Sharing | Initial | |

**Overall DORA evidence readiness, narrative summary**

**Recommended pilot (per the runtime-reachability approach)**

Pick one critical function (payment initiation is the obvious candidate for most banks), instrument the services that support it, and capture 30 days of runtime evidence. Then compare the reachable count against your existing backlog and walk the delta through internal audit before your next external review.

**Chosen pilot function & target start date**

**Completed by (signature / name)**

**Date**

**Reviewed by (internal audit)**

**Date**

Kodem

NEXT STEP

# From a backlog of findings to a record of what matters.

DORA does not mandate runtime reachability and does not prescribe a tool category. What it requires is a well-documented ICT risk management framework and a clear view of the assets, dependencies and business functions behind operational resilience. Runtime evidence is one of the most defensible ways to make that record current.

Reference: Digital Operational Resilience Act (DORA), in force 17 January 2025.