

DORA gap assessment sample

Management summary and action plan

All organisation details, evidence and findings are fictional. This illustrates a deliverable and is not a report from a completed client engagement.

The first priorities are to verify recovery of the customer portal and remove obsolete privileged access. Supplier records and system dependencies need to be completed so that decisions use a fuller view of the operating environment.

4	2	90
selected findings	P1 priorities	day planning horizon

Sample context

The hypothetical financial entity has 80 staff, a customer portal and five ICT service contracts. The example assumes that the general DORA ICT risk management framework applies, rather than the simplified framework under Article 16.

This extract covers four selected control questions. It does not cover all DORA, RTS or ITS requirements, technical security testing or an overall compliance conclusion.

Selected findings

ID and topic	Status	Priority
F01 Portal recovery	Effectiveness not verified	P1
F02 Privileged access	Gap confirmed	P1
F03 Register of information	Gap confirmed	P2
F04 System dependencies	Gap confirmed	P2

Proposed management decisions

- Confirm action owners and allocate the time and resources needed for a recovery test.
- Agree interim access-risk controls and dates for verifying completion.
- Assess progress using closure evidence; consider deferrals and residual risk separately.

First-priority findings

All organisation details, evidence and findings are fictional. This illustrates a deliverable and is not a report from a completed client engagement.

F01 Portal recovery capability is unverified

P1 | IT lead | Target within 30 days

DORA Article 12(2) and 12(6)

Evidence and observed condition. E01 - approved recovery policy: portal RTO of 4 hours and RPO of 1 hour. E02 - 30 days of successful backup logs. E03 - interview record: no recovery test report was supplied for the requested 12-month period. Successful backup records alone do not verify service recovery.

Potential impact. A disruption could prevent restoration of the service and data within the business targets. Actual recovery time is unknown in this example.

Proposed action. Agree an isolated test scenario, restore the portal data and service, record elapsed times and check data integrity. Add any failures to the action plan.

Closure criteria. A test record signed by IT and the business confirms achievement of the RTO and RPO targets and successful data checks. Missed targets remain open pending a successful retest. Any management decision on residual risk is recorded separately.

F02 A former employee's administrator account remains active

P1 | IT lead and HR | Target within 30 days

DORA Article 9(4)(c)

Evidence and observed condition. E04 - the HR record shows that the selected employee left 14 days before the review. E05 - an access export shows that the named account remains active with privileged rights. One leaver case was sampled.

Potential impact. Unnecessary access creates an opportunity for unauthorised changes or disclosure. The finding does not establish that the account was misused.

Proposed action. Remove obsolete access within 2 days, preserve relevant logs and review activity after departure. Within 30 days, agree a leaver-process control and review the remaining privileged accounts.

Closure criteria. The account is disabled, post-departure activity has been assessed, and all privileged accounts have an approved owner and business need. Evidence links the HR notification to verified IT completion.

Data and governance gaps

All organisation details, evidence and findings are fictional. This illustrates a deliverable and is not a report from a completed client engagement.

F03 Two contracts are missing from the information register

P2 | ICT supplier management owner | Target within 60 days

DORA Article 28(3)

Evidence and observed condition. E06 - the sample list of five ICT service contracts. E07 - the register of information extract covers three. Two contracts have no corresponding register entry; one entry does not identify whether the service supports a critical or important function.

Potential impact. An incomplete register makes it harder to assess dependencies and provide information to the supervisor. This sample does not assess every register field or the submission format.

Proposed action. Reconcile the full contract list to the register, add missing entries and document the basis for function classification. Assign a register owner and update triggers.

Closure criteria. All five contracts are reconciled to register entries and classification is approved by the responsible owner. Retain the reconciliation record and update responsibility. Full ITS schema validation is a separate activity.

F04 Dependencies are missing for two business services

P2 | IT architecture and business service owners | Target within 60 days

DORA Article 8(1), 8(4), 8(5) and 8(6)

Evidence and observed condition. E08 - the service and system list contains five business services. Three have system and supplier dependencies recorded; two have these fields blank. No other document explaining the missing relationships was supplied.

Potential impact. During disruption, it may be unclear which systems and suppliers are needed for recovery. Impact analysis and change assessments may rely on incomplete information.

Proposed action. Validate relationships with systems, information assets and suppliers alongside service owners. Record criticality, responsibilities and review arrangements.

Closure criteria. Key relationships and owners are approved for all five services. Review one selected recovery scenario using the updated map and document the remaining limitations.

90-day action plan

Day 0 is management approval of the plan. Timings are recommendations for this example, not statutory DORA remediation deadlines.

Timing	Action and owner	Verifiable result
Days 0-2	F02: IT removes obsolete access.	Account status and activity review record.
Days 0-7	Management and action owners approve the plan, resources and test scenario.	Confirmed ownership and test brief.
Days 8-30	F01: IT and the business test recovery. F02: IT and HR improve the access process.	Test record, account review and leaver-control evidence.
Days 31-60	F03: supplier management completes the register. F04: IT and the business approve dependencies.	Contract reconciliation and approved service map.
Days 61-90	The risk function reviews closure evidence. Management decides on remaining actions.	Closure conclusion or an open action with a revised date and risk decision.

How to read this assessment

P1 indicates potential direct impact on recovery of an important service or on privileged access. P2 indicates a data or governance gap requiring planned remediation. These are sample priorities, not an official DORA risk scale. “Gap confirmed” means an exception is visible in the sample. “Effectiveness not verified” means evidence is insufficient. The four questions are not used to calculate an overall compliance percentage. Risk acceptance alone does not demonstrate compliance with a requirement.

RTO is the recovery time objective. RPO is the recovery point objective, expressed here as the tolerated period of data loss. E01-E08 identify fictional evidence items.

References and sample limitations

Regulation (EU) 2022/2554: selected links to Articles 8, 9, 12 and 28. These references illustrate traceability and do not cover every requirement in the control area. A full assessment also establishes applicability and the relevant RTS and ITS.

EUR-Lex legal act record | Official Journal text hosted by CySEC

Discuss your assessment scope | info@glesum.it | glesum.it