Secantra
www.secantra.com

WHITEPAPER · SELF-ASSESSMENT

DORA readiness self-assessment

Five pillars, thirty-four questions, and — for every "yes" — the record that has to prove it.

A ICT risk management

B Incidents and reporting

C Resilience testing

D ICT third-party risk

E Information sharing

34 questions · 5 pillars · answer Yes / Partly / No and name the record

2026 edition · v1.0
Regulation (EU) 2022/2554 — Digital Operational Resilience Act

HOW TO USE THIS DOCUMENT

One rule: no record, no "yes"

DORA — Regulation (EU) 2022/2554 — applies to financial entities in the EU from 17 January 2025 and to the ICT third-party providers they depend on. It is organised in pillars: ICT risk management (Chapter II), ICT-related incident management and reporting (Chapter III), digital operational resilience testing (Chapter IV), managing ICT third-party risk (Chapter V) and information-sharing arrangements (Chapter VI). This self-assessment follows the same order.

Work through each pillar with the people who own it. Answer every question Yes, Partly or No, and — this is the whole point of the exercise — write down the record that proves the answer. A policy document, an approved framework adoption, an applicability decision, a control with evidence attached, a finding with an owner, a third-party record with the contract reference, a risk register entry with a treatment plan. Where there is no record, there is no "yes". That single rule turns a feelings-based questionnaire into a gap list you can act on.

The right-hand column names where such a record would live in Secantra. It is there so a team already using the product knows what to open; it is not a claim that a record in the product is sufficient on its own. Supervisors read evidence, not screenshots.

At the end there is a summary sheet and a short guide to reading the result. Keep the completed document; repeat it after every major change and at least annually — DORA expects the ICT risk framework to be reviewed on that rhythm.

The answer scale

Yes	The practice exists, is documented, and a record proves it today.
Partly	The practice exists but the record is missing, stale, or covers only some functions or systems.
No	Nothing in place, or nobody can name the owner.

Contents

PILLAR A · CHAPTER II · ARTICLES 5–16

ICT risk management

The management body owns ICT risk. Below it sits a documented ICT risk management framework and, underneath that, the identification of what the entity actually runs: functions, the ICT assets and services that support them, their dependencies, and which of them are critical or important. Everything else in DORA reads back to that inventory.

1 **Has the management body formally approved the ICT risk management framework, and does it review it — with a documented decision — at least once a year and after major ICT-related incidents?**

DORA Art. 5(2), Art. 6(5)

Record: **Board minute or approval record; framework document with version and review date**

In Secantra: **Governance document (approved, with review period)**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

2 **Are ICT risk roles assigned — a control function for ICT risk that is independent from operations, with a named owner for the framework?**

DORA Art. 5(2)–(3), Art. 6(4)

Record: **Role assignments, org chart or RACI, appointment record**

In Secantra: **Governance document; framework adoption owner**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

3 **Do the members of the management body maintain sufficient knowledge of ICT risk, with training that is actually delivered and recorded?**

DORA Art. 5(4)

Record: **Training plan and attendance record**

In Secantra: **Governance document; evidence item**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

4 **Is there a documented digital operational resilience strategy — objectives, risk tolerance, how ICT supports the business strategy — that the framework refers to?**

DORA Art. 6(8)

Record: **Strategy document referenced from the framework**

In Secantra: **Governance document**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

5 **Do you maintain a current inventory of ICT-supported business functions, the ICT assets and services that support each one, and the dependencies between them?**

DORA Art. 8(1)–(4)

Record: **Asset / service inventory with owners and relationships; a dated review**

In Secantra: **CMDB: assets IT services business solutions, structural links**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

6 **Are critical or important functions identified as such, with the criterion written down and the classification visible on the supporting assets and services?**

DORA Art. 8(1), Art. 3(22)

Record: **Criticality classification per function and per supporting asset**

In Secantra: **Business solution / IT service attributes; asset compliance links**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

7 **Are ICT risk sources, vulnerabilities and the impact of major changes reassessed on a defined cadence, with the results recorded against the affected assets or services?**

DORA Art. 8(2)–(3), (7)

Record: **Risk assessment records with date, scope and outcome**

In Secantra: **Risk register entries + assessments (score 1–25); linked assets**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

8 **Are protection and prevention controls (access, secure configuration, change, patching, data protection) documented as controls with an owner and evidence that they operate?**

DORA Art. 9

Record: **Control catalogue with owners; operating evidence per control**

In Secantra: **Controls with evidence items; requirement control mapping**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

9 **Do you have detection capabilities — monitoring, anomaly detection, alert thresholds — that cover the ICT assets supporting critical or important functions?**

DORA Art. 10

Record: **Monitoring scope list mapped to assets; alerting configuration; test of detection**

In Secantra: **Controls linked to assets; evidence items**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

10 **Are ICT business continuity, response and recovery plans in place for critical or important functions, tested at least yearly, with results and follow-ups recorded?**

DORA Art. 11, Art. 12

Record: **BC/DR plans; test reports; remediation actions**

In Secantra: **Governance documents; findings; treatment plans**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

11 **Are backup and restoration procedures defined per system, tested, and is the recovery environment segregated from production?**

DORA Art. 12(1)–(3)

Record: **Backup policy per system class; restore test evidence**

In Secantra: **Controls with evidence; asset attributes**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

12 **After a major ICT-related incident, is a post-incident review performed, and are the lessons turned into tracked corrective actions?**

DORA Art. 13(2)–(3)

Record: **Post-incident review reports; action log with owners and due dates**

In Secantra: **Findings with owner and status; treatment actions with due dates**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

13 **Do crisis communication plans exist, with responsibility for internal and external communication on major incidents assigned to a named role?**

DORA Art. 14

Record: **Communication plan; role assignment**

In Secantra: **Governance document**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

PILLAR B · CHAPTER III · ARTICLES 17–23

ICT-related incident management, classification and reporting

DORA does not ask you to run an incident tool; it asks for a process that captures, classifies and escalates ICT-related incidents consistently, and for the ability to report major incidents to the competent authority in a staged way and within short deadlines. The classification criteria and the reporting templates are set in delegated and implementing acts — the process must point at them.

14 **Is there a documented ICT-related incident management process — detection, logging, categorisation, escalation, root-cause analysis, closure — with a named process owner?**

DORA Art. 17

Record: **Process document; process owner; incident log**

In Secantra: **Governance document; controls**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

15 **Are incidents classified using the DORA criteria (clients and counterparts affected, duration, geographical spread, data losses, criticality of services, economic impact), and is the classification recorded on each incident?**

DORA Art. 18, RTS on classification

Record: **Classification procedure; classified incident records**

In Secantra: **Governance document; controls with evidence**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

16 **Can you produce the initial notification, intermediate report and final report for a major ICT-related incident within the prescribed deadlines, using the required templates?**

DORA Art. 19(1), (4)

Record: **Reporting procedure; template kit; a dry-run or a real report**

In Secantra: **Governance document; evidence item**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

17 **Is the link between an incident and the affected functions, assets and third-party services recorded, so the "affected services" fields of a report can be filled from records rather than from memory?**

DORA Art. 19, Art. 8

Record: **Incident record referencing assets / services / providers**

In Secantra: **CMDB relationships; third-party IT service links**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

18 **Where a major incident affects clients, is there a procedure to inform them without undue delay, including for significant cyber threats where relevant?**

DORA Art. 19(3)

Record: **Client communication procedure**

In Secantra: **Governance document**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

19 **Are incident data kept and analysed to spot recurring root causes, and do those analyses feed the ICT risk framework?**

DORA Art. 13(1), Art. 17(3)

Record: **Trend analysis; framework change log referencing it**

In Secantra: **Findings; risk register entries with source reference**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

PILLAR C · CHAPTER IV · ARTICLES 24–27

Digital operational resilience testing

A risk-based testing programme, proportionate to the entity, that covers the ICT systems supporting critical or important functions at least yearly, and — for entities the competent authority designates — threat-led penetration testing every three years. What matters for readiness is that the programme is documented, the scope is derived from the inventory, and every weakness found is tracked to remediation.

20 **Is there a documented digital operational resilience testing programme, risk-based and proportionate, that names the tests to be performed and how often?**

DORA Art. 24(1)–(2)

Record: **Testing programme document with an approval date**

In Secantra: **Governance document; framework adoption**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

21 **Are all ICT systems and applications supporting critical or important functions tested at least once a year, and is the scope derived from the inventory rather than from a separate list?**

DORA Art. 24(6)

Record: **Test scope traceable to the inventory; test reports per system**

In Secantra: **CMDB (critical assets / IT services); evidence items**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

22 **Are tests performed by independent parties — internal or external — and, for internal testers, is the independence documented?**

DORA Art. 24(4)

Record: **Tester independence statement or contract**

In Secantra: **Third-party record; evidence item**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

23 **Are all weaknesses, deficiencies and gaps found in testing prioritised, assigned an owner and a due date, and closed with verification?**

DORA Art. 24(5)

Record: **Findings log with status history**

In Secantra: **Findings with severity, owner and status; treatment actions with due dates**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

24 **If your entity is in scope for threat-led penetration testing (TLPT), is the three-year cycle planned, and are the critical third-party providers included?**

DORA Art. 26, Art. 27

Record: **TLPT plan; provider participation agreements**

In Secantra: **Governance document; third-party records**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

PILLAR D · CHAPTER V · ARTICLES 28–30 (AND THE REGISTER OF INFORMATION)

Managing ICT third-party risk

This is where most readiness gaps sit. DORA expects a strategy on ICT third-party risk, a register of information on all contractual arrangements with ICT third-party providers, due diligence before contracting, contracts with prescribed provisions, ongoing monitoring, and exit strategies for services supporting critical or important functions. The register is a projection of records you must already have: the provider, the service it delivers, the function it supports.

25 **Is there an approved strategy on ICT third-party risk, including a policy on the use of ICT services supporting critical or important functions?**

DORA Art. 28(2)

Record: **Strategy and policy documents with approval**

In Secantra: **Governance documents**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

26 **Do you maintain a register of information on all contractual arrangements for ICT services, at entity and — where applicable — sub-consolidated and consolidated level, in the ESA template?**

DORA Art. 28(3), ITS on the register

Record: **The register itself; the records it is built from**

In Secantra: **Third-party records □ IT services □ business solutions**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

27 **For each ICT third-party provider, is it recorded which ICT services it delivers and which functions those services support — including whether the function is critical or important?**

DORA Art. 28(3), Art. 3(22)

Record: **Provider □ service □ function links**

In Secantra: **Third-party record links; CMDB structural relationships**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

28 **Before contracting, is due diligence performed — including the assessment of ICT concentration risk and of sub-outsourcing — and is the assessment kept?**

DORA Art. 28(4), Art. 29

Record: **Due-diligence file per provider**

In Secantra: **Third-party record; evidence items; risk register entries**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

29 **Do contracts for ICT services supporting critical or important functions contain the provisions DORA prescribes (service descriptions, locations, data protection, access and audit rights, incident cooperation, exit and termination)?**

DORA Art. 30

Record: **Contract review checklist per contract; gap list**

In Secantra: **Third-party record; findings for missing clauses**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

30 **Is provider performance and risk monitored on an ongoing basis — incidents at the provider, changes in ownership or location, sub-outsourcing — with a review cadence per criticality?**

DORA Art. 28(1), (7)

Record: **Monitoring records; periodic review notes**

In Secantra: **Third-party record status and owner; risk assessments over time**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

31 **Are exit strategies in place for ICT services supporting critical or important functions, tested for feasibility, with substitutability assessed?**

DORA Art. 28(8)

Record: **Exit plan per service; substitutability assessment**

In Secantra: **Risk register entry + treatment plan; governance document**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

32 **Are the annual reports to the competent authority on new arrangements for ICT services supporting critical or important functions produced from the register rather than compiled by hand?**

DORA Art. 28(3)

Record: **Report generation procedure; last report** In Secantra: **Third-party records with contract dates**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

PILLAR E · CHAPTER VI · ARTICLE 45

Information-sharing arrangements

Voluntary, but if the entity participates in cyber threat information-sharing arrangements it must define the rules of participation, protect what is shared and notify the competent authority. Two questions cover it.

33 **If you participate in a cyber threat information-sharing arrangement, are the participation rules, confidentiality obligations and the personal-data conditions documented?**

DORA Art. 45(1)–(2)

Record: **Arrangement terms; internal participation policy**

In Secantra: **Governance document; third-party record for the community**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

34 **Has the competent authority been notified of participation (and of withdrawal), and is the notification record kept?**

DORA Art. 45(3)

Record: **Notification record**

In Secantra: **Evidence item**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

SUMMARY SHEET

Count per pillar

Transfer the counts. Then list, per pillar, the first gap you would close — the one that unblocks the most other answers.

	Pillar	Yes	Partly	No	First gap to close
A	**ICT risk management** of 13				
B	**Incidents and reporting** of 6				
C	**Resilience testing** of 5				
D	**ICT third-party risk** of 8				
E	**Information sharing** of 2				

Reading the result

Count, then look at the "No" column first

The summary sheet gives a count per pillar. Do not compute a percentage — a "Partly" on the register of information and a "Partly" on training are not the same size, and a percentage hides that. Read the "No" answers first: each is either a missing practice or a missing owner, and both are decisions, not projects.

Every "Partly" is a missing record

By construction, "Partly" means the practice exists and the proof does not. That is the cheapest gap class to close: attach the evidence, name the owner, set the review date. It is also the class that grows back fastest, which is why the record should live where the work happens, not in the questionnaire.

Three records carry most of DORA

The inventory of functions, services and assets (Art. 8), the register of information (Art. 28) and the findings log (Arts. 13, 24). If those three are current and linked to each other, most other questions turn into "which record" rather than "whether".

Repeat it

DORA expects the ICT risk framework to be reviewed at least yearly and after major incidents. Run this sheet on the same rhythm and keep the previous editions; the delta is the report your management body actually wants.

HOW THE RECORDS MAP

From "yes" to a record you can open

Secantra keeps compliance, the CMDB and risk on one record set, which is why the right-hand column of every question names one of a small number of objects. This is what they are, in the order the work usually happens:

Framework adoption	A tenant adopts a specific published version of a framework pack — DORA, NIS2, ISO/IEC 27001 Annex A. Immutable once published; adoption is version-pinned.
Applicability decision	Per requirement, per adoption: applicable, not applicable (with a reason), deferred, waived or approved as an exception — scoped tenant-wide or to a specific IT service, business solution or process. The record behind "we decided this does not apply to us".
Control	The tenant's own control, mapped to one or more requirements, with an owner and a review cadence.
Asset compliance link	The statement that a control (or a requirement) applies to a specific asset, IT service or business solution — with a status: compliant, partial, non-compliant.
Evidence item	A file or reference attached to a control, requirement or link, with a date. Evidence recency is checked; stale evidence is flagged.
Finding	A tracked gap with severity, owner and status, linked to the asset, control or requirement it concerns — from a test, an audit, an incident review or this sheet. Due dates live on the treatment actions that close it.
Governance document	Policies, frameworks, plans — versioned, approved through a configurable multi-stage flow, with a review period.
Third-party record	The provider — legal name, country, type, LEI, criticality, whether it supports a critical or important function, owner, status — and its links to the IT services it delivers and (through them) the functions it supports. For DORA, the spine of the register of information; for NIS2, of the supply-chain view.
Risk register entry	A risk with assessments over time (likelihood × impact on a 1–5 scale each), treatment plans and actions, and acceptances with expiry.

See it on your own inventory

A demo walks the DORA pack from adoption to the register of information on a sample tenant.
www.secantra.com/contact