Secantra
www.secantra.com

CHECKLIST · THIRD-PARTY RISK

DORA register of information — checklist

The register is a projection of records you must already have. Eighteen questions on whether they exist.

A Providers	**B** Services	**C** Functions	**D** Contracts	**E** Risk & exit	**F** Producing it

18 questions · 6 sections · answer Yes / Partly / No and name the record

2026 edition · v1.0
Regulation (EU) 2022/2554 — Article 28(3) and the ESA register template

HOW TO USE THIS DOCUMENT

One rule: no record, no "yes"

Article 28(3) of DORA requires every financial entity to maintain and update a register of information on all contractual arrangements for the use of ICT services provided by ICT third-party providers, distinguishing those that support critical or important functions, at entity level and — where applicable — sub-consolidated and consolidated level. The competent authority can ask for it at any time; new arrangements supporting critical or important functions are reported at least yearly. The ESAs prescribe the template through implementing technical standards.

The template is long, and it is tempting to treat it as a spreadsheet exercise. It is not: almost every column is a property of one of four records — the provider, the ICT service it delivers, the function that service supports, and the contract that binds them. If those records exist and are linked, the register is an export. If they do not, it is a quarterly project that starts again each quarter.

This checklist asks whether the records exist, in the order they usually get created. Answer Yes, Partly or No and name the record — the same rule as our other sheets: no record, no "yes". The right-hand column names where the record would live in Secantra for a team already using the product; it is not a claim that the product produces the regulatory template.

Repeat it before each yearly report and after any material change in providers or contracts.

The answer scale

Yes	The record exists for every in-scope provider / service / function, and someone owns it.
Partly	The record exists for some providers or is kept outside the system that the others live in.
No	Nothing in place, or nobody can name the owner.

Contents

SECTION A · ART. 28(3), ART. 3(19)–(21)

The ICT third-party providers

One record per provider — including intra-group providers and subcontractors that matter — with the identifiers the template asks for.

1 **Is every ICT third-party provider recorded once, with legal name, identifier (LEI where available), country and type — including intra-group service providers?**

DORA Art. 28(3)

Record: **Provider register with identifiers**

In Secantra: **Third-party records (type, status, identifiers)**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

2 **Are relevant subcontractors of critical services recorded — the material part of the ICT supply chain behind a provider?**

DORA Art. 28(3), Art. 29

Record: **Subcontractor entries linked to the primary provider**

In Secantra: **Third-party records with relationship notes**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

3 **Does each provider carry a review date and an owner, so a change of ownership, location or incident at the provider is noticed?**

DORA Art. 28(1), (7)

Record: **Provider owner; review cadence**

In Secantra: **Third-party record owner and status (under review / offboarding); risk assessments over time**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

SECTION B · ART. 28(3), ART. 3(21)

The ICT services they deliver

The template describes each ICT service, not each contract line. That means the service must exist as a record of its own, linked to the provider that delivers it.

4 **Is every ICT service delivered by a provider recorded as an IT service, linked to that provider — rather than implied by the contract title?**

DORA Art. 28(3)

Record: **IT service provider links** In Secantra: **IT services with third-party links**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

5 **Does each service carry its type, the data it processes (including personal data and its location) and where the service is provided from?**

DORA Art. 28(3), Art. 30(2)

Record: **Service attributes: type, data, locations** In Secantra: **IT service and asset records (attributes, notes)**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

6 **Where an IT service is composed of assets, are those assets linked, so criticality and incidents roll up to the service?**

DORA Art. 8(4)

Record: **Asset IT service structural links** In Secantra: **CMDB structural relationships**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

SECTION C · ART. 28(3), ART. 3(22)

The functions they support and their criticality

Criticality belongs on the function, not on the contract: the same provider can support a critical payments flow and an internal wiki. The register distinguishes arrangements supporting critical or important functions — that flag has to come from somewhere.

7 **Are business functions recorded as business solutions, each linked to the IT services it depends on?**

DORA Art. 8(1), Art. 28(3)

Record: **IT service → business solution links**

In Secantra: **CMDB: business solutions and structural links**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

8 **Is criticality classified per function with the criterion written down, so "supports a critical or important function" is derived for every service and provider?**

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

Record: **Criticality classification per function; criterion document**

In Secantra: **Business solution / asset criticality; governance document**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

9 **Can you list, for any provider, the functions it ultimately supports — and for any critical function, the providers behind it?**

DORA Art. 28(3)

Record: **Provider → service → function traversal**

In Secantra: **Third-party → IT service → business solution links**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

SECTION D · ART. 28(3), ART. 30

The contractual arrangements

The contract is the one part that should stay a legal judgement — but its reference, dates, governing law and the presence of the Article 30 provisions belong on the record.

10 **Is each contractual arrangement recorded with reference, start and end or renewal dates, notice periods and governing law, linked to the provider and to the services it covers?**

DORA Art. 28(3)

Record: **Contract references and dates per provider/ service**

In Secantra: **Evidence items (contract copies) on the third-party record — no structured contract fields in the current release**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

11 **For services supporting critical or important functions, has each contract been checked for the provisions DORA prescribes — service descriptions, locations, data protection, access and audit rights, incident cooperation, exit and termination — with the gaps tracked?**

DORA Art. 30(2)–(3)

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

In Secantra: **Findings per missing clause; evidence items**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

12 **Are cost figures (annual expense or estimated cost) available per arrangement, as the template asks?**

DORA Art. 28(3)

Record: **Cost per contract**

In Secantra: **Not in the current release — keep it in the contract file / evidence item**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

SECTION E · ART. 28(4), (8), ART. 29

Concentration, substitutability, exit

Substitutability and exit are risk statements, not paragraphs. Capture them as risks with a treatment plan and an owner, and the register's columns fill themselves.

13 **Has ICT concentration risk been assessed — one provider under several critical functions, or one location — and recorded as a risk with an owner?**

DORA Art. 29

Record: **Concentration risk assessment**

In Secantra: **Risk register entries linked to third parties**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

14 **Is substitutability assessed per service supporting a critical or important function, and is an exit strategy in place and tested for feasibility?**

DORA Art. 28(8)

Record: **Substitutability assessment; exit plan per service**

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

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

15 **Was pre-contract due diligence performed and kept for each provider of a critical service — including whether sub-outsourcing is allowed and to whom?**

DORA Art. 28(4)

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

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

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

SECTION F · ART. 28(3)

Producing and reporting the register

When A–E exist as linked records, the register is a projection. The remaining questions are about the levels it has to be produced at, and the yearly report.

16 **Can the register be produced at entity level and, where required, sub-consolidated and consolidated level, from the same records?**

DORA Art. 28(3)

Record: **Group structure mapping; register export per level**

In Secantra: **Tenant scope; exports from linked records**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

17 **Is the yearly report of new arrangements supporting critical or important functions produced from the register — with contract start dates and the criticality flag — rather than compiled by hand?**

DORA Art. 28(3)

Record: **Report generation procedure; last report**

In Secantra: **Third-party records (supports critical / important function flag); contract dates from the contract file**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

18 **Is the register kept current between reports — a change to a provider, service or function updates it the same day, with an audit trail?**

DORA Art. 28(3)

Record: **Change history on the source records**

In Secantra: **Audit events on third-party, service and solution records**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

SUMMARY SHEET

Count per section

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

	Section	Yes	Partly	No	First gap to close
A	**Providers** of 3				
B	**Services** of 3				
C	**Functions** of 3				
D	**Contracts** of 3				
E	**Risk & exit** of 3				
F	**Producing it** of 3				

Reading the result

If A–C are "No", stop there

Providers, services and functions are the spine. Without them the register is a document that decays; with them, contracts (D) and risk (E) attach to something and the register (F) is an export.

"Partly" usually means "in another system"

Procurement holds contracts, architecture holds the service map, business continuity holds criticality. The register forces them together — the cheapest way to do that is one set of linked records, not a reconciliation each quarter.

Criticality is derived, not assigned per contract

Set it on the function; let it flow down to services and providers. A contract does not know which functions depend on it — the links do.

Repeat before each report

The competent authority can ask at any time; the yearly report of new arrangements has a fixed rhythm. Run the sheet before it and keep the previous edition.

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 third-party registry from provider to service to function on a sample tenant.
www.secantra.com/contact