Secantra
www.secantra.com

CHECKLIST · SELF-CHECK

NIS2 Article 21 self-check

Governance, the ten measure areas, and reporting — thirty-two questions, each with the record that proves the answer.

A Governance	**B** Risk & policies	**C** Incident handling	**D** Continuity	**E** Supply chain	**F** Acquisition & vulns
G Effectiveness	**H** Hygiene & training	**I** Cryptography	**J** HR, access, assets	**K** MFA & comms	**L** Reporting

32 questions · 12 areas · answer Yes / Partly / No and name the record

2026 edition · v1.0
Directive (EU) 2022/2555 — NIS2

HOW TO USE THIS DOCUMENT

One rule: no record, no "yes"

NIS2 — Directive (EU) 2022/2555 — had to be transposed into national law by 17 October 2024. The operative obligations for essential and important entities sit in three articles: Article 20 (governance and accountability of the management body), Article 21 (cybersecurity risk-management measures — "appropriate and proportionate", all-hazards, covering at least the ten areas of paragraph 2) and Article 23 (reporting of significant incidents: early warning within 24 hours, incident notification within 72 hours, final report within a month). National laws largely copy them and may add detail; check yours.

This sheet follows that structure: A — governance, B to K — the ten measure areas of Article 21(2) in the Directive's order, L — reporting. Answer every question Yes, Partly or No and, for each answer, write down the record that proves it. "Appropriate and proportionate" has no meaning in the abstract — it is a statement about a specific network or information system, its exposure and the harm if it fails — so the first record on the sheet is the inventory, and most other answers point back to it.

The right-hand column names where such a record would live in Secantra, 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.

Repeat the sheet after every material change and at least annually; keep the previous editions. The difference between two of them is the report the management body needs under Article 20.

The answer scale

Yes	The measure exists, is documented, and a record proves it for the systems it should cover.
Partly	The measure exists but the record is missing, stale, or covers only some systems or sites.
No	Nothing in place, or nobody can name the owner.

Contents

AREA A · ARTICLE 20

Governance and accountability

The management body approves the cybersecurity risk-management measures, oversees their implementation and can be held liable for infringements; its members — and, regularly, the staff — follow training. Every later answer on this sheet is easier if the approval and the training are on record.

1 **Has the management body formally approved the cybersecurity risk-management measures (or the framework that defines them), with a dated, versioned decision?**

NIS2 Art. 20(1)

Record: **Approval minute; framework or policy document with version and review date**

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

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

2 **Does the management body oversee implementation — a recurring agenda item with a report on measures, incidents and open findings?**

NIS2 Art. 20(1)

Record: **Board reporting cadence; last report**

In Secantra: **Governance document; findings; posture snapshot**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

3 **Have members of the management body followed cybersecurity training, and is comparable training offered to employees on a regular basis — with attendance recorded?**

NIS2 Art. 20(2)

Record: **Training plan; attendance records**

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

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

AREA B · ARTICLE 21(2)(A)

Risk analysis and information-system security policies

The first measure area is the one the others depend on: a policy on risk analysis and information-system security, applied to a known set of systems.

4 **Do you maintain an inventory of the network and information systems in scope — assets, the services they compose, the business functions those services support — with owners?**

NIS2 Art. 21(1), 21(2)(i)

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

In Secantra: **CMDB: assets IT services business solutions; processes**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

5 **Are risks assessed against that inventory on a defined cadence, with a repeatable method and results recorded per system or service?**

NIS2 Art. 21(1), 21(2)(a)

Record: **Risk register; assessments with date, scope and score**

In Secantra: **Risk register entries + assessments (1–5 × 1–5); linked assets**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

6 **Is there an approved information-system security policy (or policy set) that names the measure areas and the systems each applies to?**

NIS2 Art. 21(2)(a)

Record: **Policy document(s) with approval and review date**

In Secantra: **Governance documents**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

7 **Have you adopted a NIS2-oriented requirement set and decided, per requirement, whether it applies, does not apply (with the reason), is deferred or waived — scoped where that is honest?**

NIS2 Art. 21(1)

Record: **Applicability decisions with reasons and scope**

In Secantra: **Framework adoption; applicability decision per requirement**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

AREA C · ARTICLE 21(2)(B)

Incident handling

A repeatable process from detection to closure, with the records that reporting under Article 23 will need.

8 **Is there a documented incident-handling process — detection, logging, classification, escalation, containment, recovery, lessons learned — with a named owner?**

NIS2 Art. 21(2)(b)

Record: **Process document; incident log**

In Secantra: **Governance document; controls**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

9 **Are incidents linked to the affected systems, services and — where relevant — suppliers, so the "affected services" part of a report comes from records?**

NIS2 Art. 21(2)(b), Art. 23

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

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

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

10 **Are lessons learned turned into tracked corrective actions with an owner and a status?**

NIS2 Art. 21(2)(b), 21(2)(f)

Record: **Post-incident reviews; action log**

In Secantra: **Findings; treatment actions with due dates**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

AREA D · ARTICLE 21(2)(C)

Business continuity, backup, disaster recovery, crisis management

Continuity is measured per system a critical function depends on — and by whether the restore was tested.

11 **Are business continuity and disaster-recovery plans in place for the services critical functions depend on, tested at least yearly, with results and follow-ups recorded?**

NIS2 Art. 21(2)(c)

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

In Secantra: **Governance documents; evidence items; findings**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

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

NIS2 Art. 21(2)(c)

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

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

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

13 **Does a crisis-management plan exist with roles, escalation and communication responsibilities assigned?**

NIS2 Art. 21(2)(c)

Record: **Crisis plan; role assignments**

In Secantra: **Governance document**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

AREA E · ARTICLE 21(2)(D), 21(3)

Supply-chain security

The measure area most entities under-record. The Directive asks you to consider the vulnerabilities specific to each direct supplier and service provider and the overall quality of their products and cybersecurity practices — a per-provider statement that only makes sense if you know which of your services each provider delivers.

14 **Is every direct supplier and service provider of network and information systems recorded, with the services it delivers and (through them) the functions it supports?**

NIS2 Art. 21(2)(d), 21(3)

Record: **Provider register with service links**

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

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

15 **Is a supplier-specific risk assessment kept per provider — vulnerabilities, security practices, secure development, concentration — and reviewed on a cadence tied to criticality?**

NIS2 Art. 21(3)

Record: **Per-provider assessment; review dates**

In Secantra: **Risk register entries linked to third parties; assessments over time**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

16 **Do contracts with providers of in-scope services carry security requirements — incident cooperation, notification, audit or assurance, exit — and is the gap list tracked?**

NIS2 Art. 21(2)(d)

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

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

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

AREA F · ARTICLE 21(2)(E)

Security in acquisition, development and maintenance; vulnerability handling

Security requirements at the point of buying or building, and a working path from a reported vulnerability to a fix.

17 **Are security requirements defined for acquiring and developing network and information systems, and applied — with evidence — to recent purchases or releases?**

NIS2 Art. 21(2)(e)

Record: **Requirements document; per-project evidence**

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

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

18 **Is there a vulnerability-handling and disclosure process — intake, triage, remediation targets by severity, coordinated disclosure — with the queue visible?**

NIS2 Art. 21(2)(e)

Record: **Process document; vulnerability queue with ages by severity**

In Secantra: **Governance document; findings by severity**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

AREA G · ARTICLE 21(2)(F)

Assessing the effectiveness of measures

The Directive asks explicitly for policies and procedures to assess whether the measures work — audits, tests, metrics — and for the results to feed back.

19 **Is there a documented approach to assessing effectiveness — internal audit, testing, metrics — with a cadence and an owner?**

NIS2 Art. 21(2)(f)

Record: **Assurance plan; last cycle's results**

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

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

20 **Do findings from audits, tests and incidents land in one log with severity, owner and status, and are they closed with verification?**

NIS2 Art. 21(2)(f)

Record: **Findings log with status history**

In Secantra: **Findings; treatment actions with due dates**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

21 **Is the posture reported to the management body derived from records — adoptions, applicability, coverage, evidence — rather than typed into a slide?**

NIS2 Art. 20(1), 21(2)(f)

Record: **Posture report with its source records; frozen snapshots for comparison**

In Secantra: **Posture snapshots (derived, immutable)**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

AREA H · ARTICLE 21(2)(G)

Basic cyber hygiene and cybersecurity training

Hygiene practices apply to systems and people; training applies to people. Both are recorded, or they did not happen.

22 **Are basic hygiene practices — patching, secure configuration baselines, least privilege, malware protection — defined as controls and applied to the in-scope systems with evidence?**

NIS2 Art. 21(2)(g)

Record: **Control catalogue; per-system evidence** In Secantra: **Controls linked to assets; evidence items**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

23 **Do all staff receive cybersecurity training on a regular basis, with completion recorded?**

NIS2 Art. 21(2)(g), Art. 20(2)

Record: **Training programme; completion records** In Secantra: **Governance document; evidence items**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

AREA I · ARTICLE 21(2)(H)

Cryptography and, where appropriate, encryption

A policy that says which data and channels are protected how — and the systems it applies to.

24 **Is there a cryptography policy — algorithms, key management, data at rest and in transit — and is it applied to the systems that store or transmit information worth protecting?**

NIS2 Art. 21(2)(h)

Record: **Cryptography policy; per-system evidence**

In Secantra: **Governance document; controls linked to assets**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

AREA J · ARTICLE 21(2)(I)

Human-resources security, access control, asset management

Three things the Directive puts in one line because they share a record: who has access to which asset, and what happens when either changes.

25 **Are joiner / mover / leaver procedures in place, with access reviewed on a cadence and the review recorded?**

NIS2 Art. 21(2)(i)

Record: **HR-security procedure; access review records** In Secantra: **Governance document; evidence items**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

26 **Is access to in-scope systems granted on least privilege and reviewed, with the identity source authoritative and synchronised?**

NIS2 Art. 21(2)(i)

Record: **Access control policy; review evidence; identity source** In Secantra: **Controls with evidence; company users synced from Entra ID**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

27 **Is the asset inventory current — owners, lifecycle status, last-seen and last-verified dates — and is it the same inventory the risk and compliance work uses?**

NIS2 Art. 21(2)(i)

Record: **Asset inventory with owners and dates; a dated review** In Secantra: **CMDB assets (owner, lifecycle, lastSeenAt / lastVerifiedAt)**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

AREA K · ARTICLE 21(2)(J)

Multi-factor authentication and secured communications

Where appropriate — which means: decided per system, and recorded where it was decided against.

28 **Is multi-factor or continuous authentication in place for the in-scope systems where appropriate, and is the "not appropriate" decision recorded per system with a reason?**

NIS2 Art. 21(2)(j)

Record: **MFA coverage per system; documented exceptions**

In Secantra: **Controls linked to assets; applicability decision with reason**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

29 **Are voice, video and text communications and emergency communication channels secured as the policy requires?**

NIS2 Art. 21(2)(j)

Record: **Communications policy; configuration evidence**

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

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

AREA L · ARTICLE 23

Reporting significant incidents

Early warning within 24 hours of becoming aware, incident notification within 72 hours, a final report within a month (an intermediate report on request); where relevant, informing recipients of the services and — for significant cyber threats — of measures they can take. It is a process with named roles, rehearsed once.

30 **Is "significant incident" defined for your entity per the Directive's criteria (severe operational disruption or financial loss; considerable damage to others), with a named role that makes the call?**

NIS2 Art. 23(3)

Record: **Classification procedure; decision owner** In Secantra: **Governance document**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

31 **Are the 24-hour early warning, 72-hour notification and one-month final report prepared as a path — who notifies the CSIRT or competent authority, with what content — and has it been rehearsed?**

NIS2 Art. 23(4)

Record: **Reporting procedure; template kit; rehearsal record** In Secantra: **Governance document; evidence item**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

32 **Where relevant, is there a procedure to inform recipients of your services about significant incidents and, for significant cyber threats, about measures they can take?**

NIS2 Art. 23(1)–(2)

Record: **Recipient communication procedure** In Secantra: **Governance document**

☐ Yes ☐ Partly ☐ No Owner: _____

Record reference / notes: _____

SUMMARY SHEET

Count per area

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

	Area	Yes	Partly	No	First gap to close
A	**Governance** of 3				
B	**Risk & policies** of 4				
C	**Incident handling** of 3				
D	**Continuity** of 3				
E	**Supply chain** of 3				
F	**Acquisition & vulns** of 2				
G	**Effectiveness** of 3				
H	**Hygiene & training** of 2				
I	**Cryptography** of 1				
J	**HR, access, assets** of 3				
K	**MFA & comms** of 2				
L	**Reporting** of 3				

Reading the result

Read the "No" column first, per measure area

The summary sheet counts per area. Do not add the areas up into a percentage — an area with one question ("Cryptography") and an area with four ("Risk and policies") are not the same size, and Article 21 does not weight them for you. A "No" is a missing measure or a missing owner; both are decisions.

"Partly" almost always means "not per system"

Most measures exist somewhere. What is usually missing is the record that says which systems they cover — and, for the rest, the recorded reason. That is the difference between a policy and an "appropriate and proportionate" measure, and it is what the inventory is for.

Two records carry most of the sheet

The inventory of network and information systems with their owners and dependencies (Article 21(2)(i)), and the findings log that effectiveness assessment feeds (Article 21(2)(f)). Keep those two current and most other questions become "which record" rather than "whether".

Repeat it

After every material change and at least annually. Keep the previous editions; the delta is the management-body report Article 20 expects, and it is also what a supervisor asks for first.

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 NIS2 pack from adoption through applicability to controls, evidence and the supply-chain view on a sample tenant. www.secantra.com/contact