NIS2 Scope Checklist

Are you in scope of NIS2 in Denmark?

27 April 2026

Table of contents

1. Introduction

The NIS2 directive (EU 2022/2555, transposed into Danish law as “Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau,” in force 1 July 2025) is the EU’s 2022 directive on network and information security. It replaces the 2016 NIS directive and significantly expands who is covered.

If you run or advise a software or SaaS company with 40-250 employees, you may be directly in scope. Or your customers may be in scope, which creates indirect compliance pressure on you even if you are not. Either way, not knowing is a liability.

This checklist has one purpose: in under five minutes, tell you whether you are likely in scope, what your classification is, and what that means in practice. It is based directly on the directive text and the Danish national transposition. It is not a substitute for legal advice.

Work through the questions in order. Each question is answerable from memory or a 30-second internal check.

2. The 12 questions

2.1. Q1: Do you have 50 or more employees?

Dansk: Har din virksomhed 50 eller flere ansatte?

(Count annual work units (AWU) per Recommendation 2003/361/EC: full-time employees count as 1 AWU; part-time and seasonal staff count as fractional AWU based on hours worked. Long-term contractors are included only if they are linked or partner enterprises under the Recommendation's ownership rules, not a flat "count all full-time contractors" rule.)

- Yes
- No
- Don't know

If Yes: You meet the minimum size threshold. Continue to Q2.

If No: You are almost certainly out of scope. Micro and small enterprises (under 50 staff AND either under €10 million annual turnover or under €10 million balance sheet total) are excluded from NIS2 obligations unless they fall into specific carve-out categories. You can stop here, but scan Q7 and Q9 to rule out size-independent triggers.

Basis: EU 2022/2555 Art. 2(1); EU Recommendation 2003/361/EC Annex Art. 2(1). Danish transposition: LOV nr. 434 af 6. maj 2025 §1 (scope), Bilag 1 (high-criticality sectors), Bilag 2 (other critical sectors).

2.2. Q2: Is your annual turnover above €10 million OR balance sheet above €10 million?

Dansk: Er din virksomheds årlige omsætning over 10 millioner euro, eller er balancesummen over 10 millioner euro?

(The SME test under Recommendation 2003/361/EC uses turnover OR balance sheet, not both. An IP-heavy SaaS with low revenue but significant balance-sheet assets can still meet this leg.)

- Yes
- No
- Don't know

If Yes (and you answered Yes to Q1): You meet the medium-sized enterprise definition. You are subject to NIS2 IF you also operate in a covered sector (Q3-Q6 below).

If No (turnover and balance sheet both below €10 million, but you still have 50+ employees): You are still in scope for the size test. The Recommendation defines "small" as fewer than 50 staff AND a financial leg below the threshold. 50 or more employees alone exits the small enterprise category, putting you in at least the medium-sized category and in scope for NIS2 if you operate in a covered sector. A 60-person SaaS with €8 million turnover meets the size test on the headcount leg alone.

Basis: EU 2022/2555 Art. 2(1); EU Recommendation 2003/361/EC Annex Art. 2(1).

2.3. Q3: Does your product or service fall into one of the Annex I categories?

Standard B2B SaaS that is NOT a managed service provider, NOT a cloud computing platform, and NOT a DNS/trust service provider is almost certainly NOT in Annex I. If that describes you, skim the list below to confirm, then skip to Q4 (Annex II).

Dansk: Leverer din virksomhed produkter eller tjenester inden for en af Bilag I-kategorierne?

NIS2 Annex I (highly critical sectors) covers: energy, transport, banking and credit institutions, financial market infrastructure, healthcare, drinking water supply, wastewater management, digital infrastructure (DNS providers, TLD name registries, cloud computing providers, data centre operators, content delivery networks, internet exchange points, trust service providers, providers of public electronic communications networks and publicly available electronic communications services), ICT service management B2B (MSPs, MSSPs), public administration, and space (ground infrastructure operators).

- Yes, my company operates in one of these sectors
- No
- Partially: we serve these sectors but are not in them ourselves

If Yes: You are in scope as an Annex I entity. Your classification (essential vs important entity) depends on size. Continue to Q10.

If No: Continue to Q4.

If Partially: This is the supply-chain question, and it matters. If your customers are in Annex I sectors, see Q9.

Basis: EU 2022/2555 Annex I; NIS2-loven Bilag 1.

2.4. Q4: Does your product or service fall into one of the Annex II categories?

Dansk: Leverer din virksomhed produkter eller tjenester inden for en af Bilag II-kategorierne?

NIS2 Annex II (other critical sectors) covers: postal and courier services, waste management, manufacture, production and distribution of chemicals, production, processing and distribution of food, manufacturing of medical devices and in vitro diagnostic medical devices, computer, electronic and optical products, electrical equipment, machinery and equipment n.e.c., motor vehicles, other transport equipment, digital providers (online marketplaces, online search engines, social networking platforms), and research organisations.

- Yes, my company operates in one of these sectors
- No
- Don’t know

If Yes: You are in scope as an Annex II entity (important entity) if you also meet the size thresholds. Continue to Q10.

If No: Continue to Q5.

Basis: EU 2022/2555 Annex II; NIS2-loven Bilag 2.

2.5. Q5: Are you a cloud computing service provider, data centre operator, or content delivery network?

Dansk: Driver din virksomhed cloud-tjenester, datacentre eller indholdslevering (CDN)?

- Yes
- No
- Don’t know

If Yes: You fall under Annex I (digital infrastructure) regardless of which other sector you consider yourself in. Cloud computing service providers are explicitly named in Annex I, point 8. Note: cloud provision is sector-based, not size-independent like trust services in Q8. A sub-threshold cloud provider (under 50 employees AND under €10 million turnover or balance sheet) is out of scope altogether. Above the threshold, your size determines whether you are essential or important.

If No: Continue to Q6.

Basis: EU 2022/2555 Annex I, point 8.

2.6. Q6: Are you a managed service provider (MSP) or managed security service provider (MSSP)?

Dansk: Leverer din virksomhed managed services (IT-drift, IT-support, sikkerhedstjenester) til andre virksomheder?

An MSP under NIS2 is a company that provides ongoing management, monitoring, or operation of IT systems or infrastructure on behalf of other businesses, typically with privileged access to customer environments. The operative test is operational, not what your website says: if you hold admin credentials for customer systems, monitor customer networks, or configure and maintain customer infrastructure on a recurring basis, you are likely an MSP under NIS2.

- Yes, my company provides managed IT services with privileged access to customer environments
- No, we provide software that customers operate themselves
- Hybrid: we have both a SaaS product and a managed service offering

If Yes: You fall under Annex I, ICT service management (B2B). MSPs default to important entity status unless they exceed 250 employees, OR €50 million annual turnover, OR €43 million annual balance sheet total, in which case they are essential entities.

If No (standard SaaS): Your classification depends on which sector your customers are in. See Q7 and Q8. Standard multi-tenant SaaS where customers operate the software themselves may fall

outside direct scope if the company itself does not meet the sector criteria. But read Q9 on supply-chain obligations before concluding you are out of scope.

If Hybrid: You have dual classification risk. The managed service component places you in Annex I. Assess both strands separately.

Basis: EU 2022/2555 Annex I §11 (ICT service management B2B) and Art. 6(37) (definition of managed service provider).

2.7. Q7: Are you a provider of public electronic communications networks or services?

Dansk: Leverer din virksomhed offentlige elektroniske kommunikationsnet eller -tjenester?

This covers telecoms operators, internet access providers, and providers of publicly available voice or data services. It does not cover private corporate networks.

- Yes
- No
- Don’t know

If Yes: You are covered regardless of company size. Public electronic communications providers are one of the size-independent categories under Art. 2(2)(a). Note: any entity that is the sole provider of an essential service in a Member State is also size-independently in scope, regardless of sector. This applies to very few organisations, but if you are the only provider of an essential service in Denmark, it is relevant.

If No: Continue to Q8.

Basis: EU 2022/2555 Art. 2(2)(a).

2.8. Q8: Do you provide qualified trust services, domain name registry services, or DNS resolution?

Dansk: Leverer din virksomhed kvalificerede tillidstjenester (fx e-signatur, e-segl), TLD-registrering eller DNS-opløsning?

Trust services under EU 910/2014 (eIDAS) include electronic signatures, electronic seals, timestamps, and certificate issuance. DNS providers are any company operating recursive or authoritative DNS services for third parties.

- Yes
- No
- Don’t know

If Yes: Two rules apply. First, all trust service providers (qualified or not) are in scope regardless of size under Art. 2(2)(b). Second, qualified trust service providers, DNS service providers, and TLD name registries are additionally classified as essential entities regardless of size under Art. 3(1)(b) and

3(1)(c). If you provide non-qualified trust services, you are still in scope; your essential or important classification depends on headcount and financials.

If No: Continue to Q9.

Basis: EU 2022/2555 Art. 2(2)(b), Art. 3(1)(b), Art. 3(1)(c).

2.9. Q9: Do your customers include companies or public bodies that are themselves in scope for NIS2?

Dansk: Har din virksomhed kunder, som selv er omfattet af NIS2-loven (fx energiselskaber, hospitaler, offentlige myndigheder, banker)?

This question matters even if you are not directly in scope. NIS2 Art. 21(2)(d) requires covered entities to manage cybersecurity risks in their supply chain, including their ICT suppliers. If your customers are in scope, they are required to impose minimum security requirements on you through their supplier contracts.

- Yes, a significant portion of our customers are in NIS2-covered sectors
- Some, but it is not central to our business
- No

If Yes: You are not directly obligated by NIS2, but you will face contractual pressure to demonstrate equivalent cybersecurity practices. Customers in scope for NIS2 who cannot verify your security posture face enforcement risk themselves. Practically: supplier security questionnaires, contract clauses requiring incident notification windows, demands for ISO 27001 certification or SOC 2 reports. Your customers are legally required to manage this.

If Some: The same applies for those customer relationships. Scope it by revenue concentration.

If No: You are likely out of scope entirely. Confirm with Q10 and the scoring guide below.

Basis: EU 2022/2555 Art. 21(2)(d); Art. 21(3).

2.10. Q10: Are you headquartered or registered in Denmark, or do you provide services to customers in Denmark or elsewhere in the EU?

Dansk: Er din virksomhed hjemmehørende i Danmark, eller leverer I tjenester til kunder i Danmark eller andre EU-lande?

Three jurisdictional cases. (i) Single-country Danish entity: Danish NIS2-loven applies (Art. 26(1)). (ii) Entity established in multiple EU member states: jurisdiction follows your main establishment, defined as where cybersecurity risk-management decisions are predominantly taken (Art. 26(2)). (iii) Entity not established in the EU at all but offering services into the EU: you must designate an EU representative, and that representative's member state's law applies (Art. 26(4)).

- My company is incorporated and primarily operates in Denmark
- Incorporated elsewhere but with significant operations or customers in Denmark/EU
- Operating entirely outside the EU

If Denmark: Danish NIS2-loven (LOV nr. 434 af 6. maj 2025) applies directly. You register via virk.dk under SAMSIK's NIS2 registration self-service. The required fields are entity name, CVR, sector and subsector per Bilag 1-2, contact details (email, IP ranges, phone), the EU member states where you provide services, and for certain digital entities the HQ address. The self-registration deadline was 1 October 2025. If you missed it, see Section 4 below.

If EU but not Denmark: The member state where you have your principal establishment is the competent authority. You are not subject to Danish law specifically, but you are subject to the equivalent national transposition where you are established.

If outside EU entirely: You are not directly subject to NIS2 unless you provide services to EU entities that qualify and designate you as a critical supplier.

Basis: EU 2022/2555 Art. 26 (jurisdiction); LOV nr. 434 af 6. maj 2025 §2.

2.11. Q11: Have your customers started sending you supplier security questionnaires or asking you to sign data processing or security addenda referencing NIS2?

Dansk: Har I begyndt at modtage leverandørspørgeskemaer eller kontrakttillæg fra kunder, som refererer til NIS2?

This is a market-signal question, not a legal one. But it is a fast proxy for whether you are already inside your customers' Art. 21 supply-chain assessment scope.

- Yes, in the last 12 months
- No
- We have not tracked this

If Yes: The commercial pressure is already real. Regardless of your direct legal exposure, your customers have decided you are a relevant supplier for NIS2 purposes. This creates a de facto compliance requirement because losing a contract is a harder consequence than a regulator's letter.

If No: Either your customers have not started their own NIS2 programs yet, or you are genuinely outside their supply chain risk perimeter. Neither conclusion is permanent.

Basis: Commercial intelligence; EU 2022/2555 Art. 21(2)(d) rationale.

2.12. Q11.5: Are you a SaaS sub-processor where your direct contract is with an integrator or reseller, not the regulated end-customer?

Dansk: Er din virksomhed underleverandør, hvor jeres direkte kontrakt er med en integrator eller forhandler, ikke med den NIS2-omfattede slutkunde?

This is a common B2B SaaS architecture: you provide software to an integrator (system house, MSP, or reseller) who then deploys it for an end-customer who is themselves NIS2-covered. Your contract is with the integrator, but the operational risk lives at the end-customer level.

- Yes, this matches our delivery model

- No, we contract directly with the regulated entity
- Mixed: both architectures exist in our portfolio

If Yes: The NIS2 Art. 21(2)(d) supply-chain obligation flows from the regulated end-customer to their direct supplier (the integrator), and from the integrator to you as their sub-supplier. You will face contractual security questionnaires from the integrator that pass through the end-customer's NIS2 obligations. Practically: your DPA with the integrator needs to include pass-through of NIS2-relevant security clauses, and your incident notification windows need to match what the integrator owes their end-customer (which may be 24 to 48 hours where the end-customer is NIS2-covered).

If No: Standard direct-contract handling per Q9.

If Mixed: Run both Q9 and this Q11.5 logic for the relevant portions of your customer base.

Basis: EU 2022/2555 Art. 21(2)(d); Art. 21(3) on flow-down to the supply chain; standard sub-processor architecture under GDPR Art. 28(4).

2.13. Q12: Are you regulated under DORA (Digital Operational Resilience Act, EU 2022/2554)?

Dansk: Er din virksomhed underlagt DORA (EU 2022/2554 om digital operationel modstandsdygtighed for den finansielle sektor)?

DORA covers banks, insurance companies, investment firms, payment institutions, crypto asset service providers, and the critical ICT service providers that serve them. DORA entered into application on 17 January 2025.

- Yes, we are a financial entity under DORA or a critical ICT third-party service provider to financial entities
- No
- Don't know

If Yes: DORA functions as lex specialis over NIS2 for the specific provisions on cybersecurity risk-management measures (NIS2 Art. 21) and incident notification (NIS2 Art. 23) — these are explicitly displaced under NIS2 Art. 4(1). Other NIS2 obligations are not addressed by Art. 4(1). Registration with the Danish competent authority almost certainly still applies. NIS2 Art. 20 management-body governance is most likely additionally binding given DORA Art. 5 covers similar ground, but the interaction is a live interpretive question rather than a settled rule. Take legal advice before assuming Art. 20 NIS2 governance can be discharged purely through DORA Art. 5 compliance.

If No: Continue to the scoring guide.

Basis: EU 2022/2554 (DORA) Recital 16; EU 2022/2555 Art. 4(1).

3. Scoring and interpretation guide

Work through this after completing all 12 questions.

3.1. Essential entity (Væsentlig enhed)

You are likely classified as an **essential entity** if ALL of the following apply:

- Q1: 250 or more employees, OR
- Q2: Annual turnover above €50 million (or balance sheet above €43 million)
- AND you answered Yes to Q3 (Annex I sector), Q5 (cloud/data centre/CDN), Q6 (MSP/MSSP), Q7 (public communications), or Q8 (trust/DNS services)
- AND Q10 confirms you are established in Denmark or the relevant EU member state

What this means: You face the stricter supervision tier. Maximum administrative fines of at least €10 million or 2% of global annual turnover, whichever is higher. (NIS2 sets the ceiling Member States must allow regulators to impose; the actual fine in any given case depends on the circumstances and the national implementing rules.) Styrelsen for Samfundssikkerhed (samsik.dk) is the primary NIS2 competent authority in Denmark; sector regulators supervise their own sectors. Under NIS2-loven, management is personally liable for approving cybersecurity measures. Not the security team. Management.

Basis: EU 2022/2555 Art. 3(1), Art. 32, Art. 34(4).

3.2. Important entity (Vigtig enhed)

You are likely classified as an **important entity** if ALL of the following apply:

- Q1: 50 or more employees, OR
- Q2: Annual turnover above €10 million (or balance sheet above €10 million)
- AND you answered Yes to Q3 (Annex I sector) OR Q4 (Annex II sector) OR Q6 (MSP/MSSP)
- AND you do NOT meet the essential entity size thresholds above
- AND Q10 confirms Danish or EU establishment

What this means: You face reactive supervision (regulators investigate when incidents occur or complaints are filed). Maximum administrative fines of at least €7 million or 1.4% of global annual turnover, whichever is higher (same caveat as Section 3.1: this is the ceiling Member States must allow, not a guaranteed minimum imposed amount). The same 10 security measures under Art. 21 apply; the difference is primarily in supervision intensity and the fine ceiling.

Basis: EU 2022/2555 Art. 3(2), Art. 33, Art. 34(3).

3.3. Supply-chain obligation only (Indirekte forpligtelse via forsyningskæde)

You are likely in a **supply-chain obligation position** (not directly regulated, but commercially and contractually bound) if:

- Q9: Yes, your customers are NIS2-covered entities
- AND you answered No or borderline on Q3-Q8 (not in a covered sector yourself)
- OR you are below the size thresholds in Q1-Q2

What this means: see Q9 for the full description of how supply-chain pressure flows. Short version: NIS2 does not directly bind you, but covered customers will pass through their Art. 21(2)(d) obligations contractually. Non-compliance risks contract loss, not regulatory fines.

Basis: EU 2022/2555 Art. 21(2)(d), Art. 21(3).

3.4. DORA track (Finansiel regulering via lex specialis)

You are on the **DORA track** (not NIS2) if Q12 is Yes.

What this means: Run your cybersecurity and operational resilience program through DORA, not NIS2. The obligations overlap substantially; the practical difference is which regulator supervises you and which specific reporting deadlines and technical standards apply.

Basis: EU 2022/2554 Recital 16; EU 2022/2555 Art. 4(1).

3.5. Likely out of scope

You are likely **out of scope** if:

- Q1: Under 50 employees AND Q2: Under €10 million turnover AND under €10 million balance sheet total
- AND you answered No to Q3-Q9 (no covered sector, no size-independent trigger, no significant NIS2 customer base)
- AND Q12: No DORA obligation

What this means: NIS2 does not apply to you today. This can change if you grow past the thresholds or if your customer mix shifts toward covered sectors. Keep a note of when you last checked.

Important: Likely out of scope is not a legal opinion. If any question produced a Don’t know answer, get a definitive answer before concluding you are out.

Basis: EU 2022/2555 Art. 2(1); LOV nr. 434 af 6. maj 2025 §1.

4. If you are in scope, three things to do in the next 30 days

1. Register. If you are in scope and have not already registered, the self-registration deadline was 1 October 2025 via virk.dk under SAMSIK's NIS2 self-service. You are late. Register now. The registration requires your CVR, your sector and subsector per Bilag 1-2, contact details (email, phone, IP ranges), and the EU member states where you provide services. Use the NIS2tjek tool at nis2tjek.sikkerdigital.dk to confirm your sector classification before you register.

2. Run a gap assessment against Art. 21(2). NIS2 Art. 21(2) lists 10 specific measures (a) through (j): (a) risk-analysis and information-system security policies, (b) incident handling, (c) business continuity (backup, DR, crisis management), (d) supply-chain security, (e) security in acquisition, development and maintenance of network and information systems including vulnerability handling, (f) policies and procedures to assess effectiveness of cybersecurity risk-management measures, (g) basic cyber hygiene practices and security training, (h) policies on cryptography and encryption, (i) human-resources security, access-control and asset management, (j) multi-factor or continuous authentication and secured communications. Most B2B SaaS companies with an engineering team already do parts of (b), (c), (i), and (j). The gaps are typically in (d) supply-chain documentation, (e) SSDLC and vulnerability disclosure, (f) effectiveness assessment, and management-level approval of the security policy. A structured internal review against (a) through (j) tells you where you actually stand.

3. Brief your board or senior management AND schedule training. NIS2-loven holds management bodies personally liable for approving and overseeing cybersecurity measures. "The security team handles it" is not a compliant posture. Management needs to approve a written cybersecurity policy, receive regular reports, AND follow cybersecurity training. Art. 20(2) NIS2 requires members of management bodies to follow training sufficient to identify risks and assess security measures. The Directive prescribes no minimum duration, frequency, or assessment standard; LOV nr. 434 af 6. maj 2025 implements the obligation as written.

Where to get help: You can run the gap assessment internally using SAMSIK guidance at samsik.dk. (CFCS / Center for Cybersikkerhed was absorbed into Styrelsen for Samfundssikkerhed in January 2025; cfcs.dk now redirects to samsik.dk.) Dansk Industri has a published NIS2 guide. You can also hire a compliance consultant or a law firm with a cybersecurity practice. Accel Comply runs structured readiness assessments specifically for B2B software and SaaS companies. If you want an external set of eyes rather than doing it in-house, that is the conversation to have.

Basis: EU 2022/2555 Art. 20(1), Art. 21.

5. Sources and further reading

Primary sources:

- EU 2022/2555 (NIS2 Directive), full text: eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555
- Danish national transposition, Styrelsen for Samfundssikkerhed: samsik.dk/nis2
- Dansk FAQ on NIS2 scope and obligations: samsik.dk/nis2/faq
- NIS2tjek (Danish self-assessment tool): nis2tjek.sikkerdigital.dk
- EU Recommendation 2003/361/EC (SME size definitions): eur-lex.europa.eu/LexUriServ

Third-party reads:

- Bird and Bird, NIS2 Denmark overview: twobirds.com
- Kemp IT Law, MSP and ICT service management classification: kempitlaw.com
- ISMS.online, SaaS and digital service provider scope analysis: isms.online