TechSuit · EU & cross-border GRC

The 3-Minute NIS2 & Cross-Border GRC Applicability Calculator

Determine your scope, liability, and compliance baseline under NIS2, Spain's ENS, Greece's Law 5160/2024, and Israel's Protection of Privacy Law.

The risk you’re actually carrying

NIS2 (Directive (EU) 2022/2555) changed who is personally on the hook when a business gets breached. Under **Article 20**, your management body - the owner, the directors, the people who sign off on budget - has to approve your cybersecurity risk-management measures, oversee that they're actually implemented, and complete cybersecurity training. If your organisation infringes its Article 21 security duties because leadership never approved a real risk-management plan, that's a governance failure the law now points at by name.

The fines sit in a different article, **Article 34**, and they're large enough to change a board conversation:

Entity class	Maximum fine
Essential entity	€10,000,000 or 2% of total worldwide annual turnover, whichever is higher
Important entity	€7,000,000 or 1.4% of total worldwide annual turnover, whichever is higher

Those are EU-wide floors, not ceilings. Some member states set their own numbers higher in national law. Competent authorities can also order a temporary ban on a member of senior management holding a management position, on top of the fine.

The part most small businesses miss: size doesn't make you safe. Article 21(2)(d) requires regulated entities to manage the security of their supply chain, including the relationship with their direct suppliers and service providers. In practice, a regulated hospital, bank, or energy company now has to ask its vendors - including you, if you're their IT provider, software vendor, or logistics partner - to demonstrate baseline security. You don't have to be "in scope" of NIS2 yourself to feel its weight. You just have to sell to someone who is.

That's the real reason this calculator exists. Most small businesses ask "does NIS2 apply to me?" and stop at the first no. The better question is "who in my customer list is regulated, and what are they about to ask me for?"

Where enforcement actually stands. NIS2's transposition deadline was 17 October 2024, but adoption across the EU has been uneven - only a handful of member states met that date, and the European Commission has referred several, including Spain, to the Court of Justice of the EU over incomplete transposition. Practically: don't assume your country's final rules are settled, and don't assume they aren't. Check your national transposition law before you finalise a compliance budget, and treat this guide as the map, not the final word on your specific obligations.

Step 1: The sector and jurisdiction test

NIS2 splits regulated sectors into two annexes. Which one you sit in decides whether you could be an "essential" or an "important" entity - and how strict the supervision is.

Annex I - sectors of high criticality

- Energy (electricity, oil, gas, hydrogen, district heating)
- Transport (air, rail, water, road)
- Banking
- Financial market infrastructures
- Health (hospitals, reference laboratories, medical device and pharmaceutical manufacturers)
- Drinking water
- Waste water
- Digital infrastructure (data centres, cloud providers, DNS providers, TLD registries, IXPs, trust service providers)
- **ICT service management (business-to-business)** - this is the line that pulls in MSPs and MSSPs directly
- Public administration
- Space

Annex II - other critical sectors

- Postal and courier services
- Waste management
- Chemicals (manufacture, production, distribution)
- Food (production, processing, wholesale distribution)
- Manufacturing (medical devices, electronics, machinery, motor vehicles, other transport equipment)
- Digital providers (online marketplaces, online search engines, social networking platforms)
- Research organisations

If your business sits in either list, move to Step 2. If it doesn't, don't close the tab yet - the supply chain effect in Step 3 may still apply, and the jurisdictional notes below matter if you operate in Greece, Spain, or Israel.

Jurisdiction notes for cross-border operators

Greece - Law 5160/2024. Greece transposed NIS2 through Law 5160/2024, and regulated entities register with the National Cybersecurity Authority (NCSA) through its dedicated platform, linked from **cyber.gov.gr**. If you're in scope, treat registration as a standing obligation, not a one-time task - the NCSA has already run one registration window and continues to process new entrants. Confirm your current registration and incident-reporting contact details directly on cyber.gov.gr before you need them; official contact channels are exactly the kind of detail worth re-checking at the time, not

memorising from a PDF.

Spain - Real Decreto 311/2022 (Esquema Nacional de Seguridad). If you provide technology, software, or services to any part of the Spanish public sector, RD 311/2022 requires your systems to meet one of three ENS security categories, assessed across five dimensions: confidentiality, integrity, availability, traceability, and authenticity.

ENS category	What it signals
BASICA	Limited, recoverable harm if something goes wrong. Typical of informational or low-sensitivity systems.
MEDIA	Serious but recoverable harm. Covers most systems that process personal data or deliver an administrative service.
ALTA	Very serious or irreparable harm. Reserved for critical or highly protected information and essential services.

Public-sector contracts increasingly write ENS compliance directly into the tender specification - if you sell to a Spanish public body, expect to be asked which category you meet and to show evidence of it.

Israel - Protection of Privacy Law (Amendment 13). Amendment 13 took effect on 14 August 2025 and is the biggest change to Israeli privacy law in decades. Two thresholds matter for a growing business, and they're easy to conflate:

- A database used mainly for direct marketing or data brokerage, or held by a public body, generally needs full **registration** with the Privacy Protection Authority once it covers more than **10,000** individuals.
- A database holding **highly sensitive data** on more than **100,000** individuals triggers a lighter **notification** duty instead of full registration, including a **Database Definition Document** and the details of your appointed privacy officer.

Separately, the underlying Data Security Regulations (5777-2017) grade every database as Basic, Medium, or High based on the type of data it holds and how many people can access it - record count alone doesn't decide your tier. If you're not sure which bucket you're in, that's a five-minute conversation with a privacy lawyer, not a guess.

Step 2: The size-cap rule and out-of-scope exceptions

Assuming you sit in Annex I or Annex II, NIS2 applies the EU's standard size-cap test.

In scope by size:

- **Medium enterprise** - 50 or more employees, or annual turnover/balance sheet total above €10 million
- **Large enterprise** - 250 or more employees, or annual turnover above €50 million

Large enterprises in Annex I sectors are generally treated as **essential entities**. Medium enterprises in Annex I, and medium or large enterprises in Annex II, are generally treated as **important entities**. Micro and small businesses below the size cap are, as a general rule, out of scope.

The exceptions that ignore size entirely. A small number of entity types are regulated under NIS2 no matter how small they are, because the service itself is critical infrastructure:

- Providers of public electronic communications networks or services
- Trust service providers
- Top-level domain (TLD) name registries and DNS service providers
- Public administration entities of central government
- Any entity that is the **sole provider** of a service in a member state that's essential for maintaining critical societal or economic activity
- Entities whose disruption could have a significant impact on public safety, public security, or public health

If none of those describe you and you're under the size cap, the direct-regulation door closes. Step 3 is where most small businesses actually live.

Step 3: The compliance status scoring matrix

Read down until a row matches your business:

Your profile	Your status	What it means
Annex I sector + medium/large enterprise	**Essential entity**	Proactive supervision. Regulators can audit you before an incident happens, not just after.
Annex II sector + medium/large enterprise	**Important entity**	Reactive (ex-post) supervision. Regulators act mainly after an incident or complaint.
Small/micro enterprise + one of the size-independent exceptions	**Regulated entity**	Same duties as above, size doesn't exempt you.
Small/micro enterprise, no exception, but you sell to a regulated Annex I or II entity	**Sub-regulated vendor**	Not directly regulated, but Article 21(2)(d) means your customer's security team will ask you to prove baseline controls before renewing your contract.
Small/micro enterprise, no exception, no regulated customers	**Out of scope for now**	Worth re-checking annually - a single new enterprise client can put you in the vendor row above.

Most small and medium businesses we work with land in the fourth row. That's not a loophole, it's the design of the directive - NIS2 was built to push baseline security down the supply chain, not just onto the largest companies.

Remediation and next steps

Whatever row you landed in, the next move is the same: find out where your actual gaps are before a customer, an auditor, or an incident finds them for you.

1. **Map your Article 21 risk-management measures against what you actually have today.** Article 21 sets out ten categories - risk analysis, incident handling, business continuity, supply chain security, secure development, policies for testing effectiveness, basic cyber hygiene and training, cryptography, HR security and access control, and multi-factor authentication. Most small businesses have some of these informally and none of them documented.
2. **If you're a sub-regulated vendor, get ahead of the questionnaire.** Larger clients are starting to send security questionnaires before they'll renew a contract. Answering "yes, and here's the evidence" instead of scrambling is the difference between keeping the account and losing it to a competitor who prepared first.
3. **Pick one framework to run the whole programme through**, instead of chasing NIS2, ENS, and ISO 27001 as three separate projects with three separate spreadsheets.

That's what we actually do for clients. TechSuit runs a worksheet-driven GRC audit that maps your real infrastructure, straight from your endpoints and identity setup, onto the **CIS Controls v8.1** framework. CIS Controls is the technical hub that satisfies NIS2's Article 21 baseline, Spain's ENS, and ISO 27001 at the same time - you implement the controls once and the paperwork for all three follows from the same evidence.

Book a free 30-minute call and we'll walk through where you actually stand, in plain language, with no obligation to sign anything.