NIS2 on One Page

Quick-reference cheat sheet · Directive (EU) 2022/2555 · **null-packet** · not legal advice, verify against your national transposition

Who's in scope

Default: medium+ enterprise (≥50 staff **or** >€10m turnover/balance sheet) in a listed sector. **Regardless of size:** telecom, trust services, DNS/TLD, sole/critical providers. *"Too small" is the most common wrong answer, MSPs are in.*

	Essential	Important
Who	Large in Annex I + size-independent	Medium in Annex I; Annex II
Supervision	Proactive (audits/inspections)	Ex-post (after evidence/incident)
Max fine	€10m or **2%** global turnover	€7m or **1.4%** global turnover

Obligations are the **same** for both, only supervision and fines differ.

Governance (Art. 20), the personal one

Management **approves** measures · **oversees** them · gets **trained** · can be held **liable**. → Keep a **dated management approval** on record.

The 10 measures (Art. 21), all-hazards, proportionate

	Measure	The one thing to get right
`a`	Risk analysis & IS policy	A register that's actually reviewed
`b`	Incident handling	IR plan with the reporting clock wired in
`c`	BC / backup / DR	Test **restores**, not just backup jobs
`d`	Supply chain security	Tier suppliers; your MSP is a critical risk
`e`	Secure dev & vuln handling	Patch by risk (KEV), across the whole estate
`f`	Assess effectiveness	**Test** controls, don't just have them
`g`	Cyber hygiene & training	Onboarding + annual, with records
`h`	Cryptography & encryption	Disk + transit + backups; a written policy
`i`	HR security / access / assets	JML, access reviews, an asset register
`j`	MFA & secure comms	MFA everywhere feasible; out-of-band channel

The reporting clock (Art. 23), from AWARENESS

`24 hours`	EARLY WARNING, malicious? cross-border?
`72 hours`	NOTIFICATION, severity, impact, IOCs
`on ask`	INTERMEDIATE, status updates
`1 month`	FINAL REPORT, root cause, mitigations

Significant = severe operational disruption / financial loss, or considerable damage to others. If personal data: GDPR 72h to the DPA runs *in parallel*.

Do this first (in order)

1. Confirm scope + Essential/Important · register with the authority
2. Stand up governance (approval + quarterly cadence + director training)
3. Asset & supplier registers
4. Risk assessment
5. Incident readiness + reporting templates + CSIRT contact
6. Close control gaps by risk
7. Evidence pack + management report

Framework shortcut
Already run one of these? NIS2 maps onto it, don't start over:
ISO/IEC 27001:2022 · **NIST CSF 2.0** · **CIS Controls v8**.