

NIS2 technical gap checklist

Pikas Systems · 26 Aug 2026 · Not legal advice. Fill Have? with have / gap / n/a.

Map from Directive (EU) 2022/2555 Arts. 20, 21 and 23 to evidence your platform can produce. If a reviewer who does not own the system cannot open the path in five minutes, it is a gap. If evidence is not in git, write the system of record.

Article 21(2)

ART.	MEASURE	EVIDENCE IN THE REPO	HAVE?
21(2)(a)	Risk analysis & IS security policies	docs/security/risk-register.md — owners, last review, residual risk accepted by name.	
21(2)(b)	Incident handling	docs/runbooks/incident.md executed. On-call routing in code. Ticket captures detect / aware / impact / IoCs.	
21(2)(c)	Continuity, backup, DR, crisis	Backups in Terraform/Pulumi. docs/runbooks/restore.md. Last restore: what, how long, who authorised.	
21(2)(d)	Supply chain, direct suppliers	docs/suppliers.md. SBOM per release. Signed artifacts, pinned digests. Vendor access federated.	
21(2)(e)	Acquisition, development, vuln handling	One path to production. Vuln tickets with SLA. SECURITY.md disclosure contact.	
21(2)(f)	Effectiveness assessment	Restore / failover / rotation drills. docs/audits/ with date, finding, owner, due date.	
21(2)(g)	Hygiene and training	Baseline as code. Training records for management (Art. 20(2)) and staff.	
21(2)(h)	Cryptography / encryption	TLS and encryption-at-rest as module defaults. Key lifecycle. No secrets in state or CI vars.	
21(2)(i)	HR security, access, assets	Joiner-mover-leaver in IdP groups as code. Console users and access-key age.	
21(2)(j)	MFA; secured comms; emergency comms	MFA at IdP. OIDC per CI job. Audited break-glass. Emergency channel that survives losing Slack.	

Article 23 — notification clock

The legal clock starts when you become aware. If a customer is first to know, you can still file in 24h — and you have already failed the detection duty that makes the clock useful.

ART.	MEASURE	EVIDENCE IN THE REPO	HAVE?
23(4)(a)	Early warning, 24h	Alert that pages on customer-visible impact. Runbook: who files, which CSIRT, which template. Detect → aware is measured.	
23(4)(b)	Notification, 72h	Same template plus severity, impact, IoCs. Owner who can file without a board meeting.	

ART .	MEASURE	EVIDENCE IN THE REPO	HAVE?
23(4)(d)	Final report, 1 month	Timeline from logs you still have. Retention long enough to reconstruct a month.	
23(1)	Notify service recipients	Customer-comms template and the list of who gets it.	

Article 20 — management

ART .	MEASURE	EVIDENCE IN THE REPO	HAVE?
20(1)	Management approves, oversees, can be liable	Named approver on the risk register. Recurring board pack generated from production sources.	
20(2)	Management cybersecurity training	Date of last session, attendance, material.	

Board pack: open incidents · MTTD/MTTR and 24h drill · vulns past SLA · last restore · privileged access and MFA · unsigned artifacts / unnamed suppliers · training · residual risks accepted this quarter.

Directive (EU) 2022/2555 · Implementing Regulation (EU) 2024/2690 (digital infrastructure / ICT, direct application).
Send the filled last column plus two lines about your stack to hola@pikas.systems.