NIS2 Management Training Log

Article 20(2), Directive (EU) 2022/2555 · national transpositions incl. § 38 Abs. 3 BSIG (DE)

FREE TEMPLATE — XLSX · PDF · MD | Version 1.0 · Updated 2026-07-21

What the workbook contains

Management Body Register	One row per member of the management body: name, role, governing body, appointment date, whether the member is in scope of the Article 20 duty (with justification), status, and two computed columns — latest completed session and next training due. Auditors sample training records against exactly this list; overdue members highlight automatically.
Training Log	One row per member per session: session title, provider and provider type, date, duration in hours, format, which of the three Article 20(2) objectives the content covered (identify risks / assess risk-management practices / impact on services), the renewal interval, a computed next-due date, the evidence reference (certificate, signed attendance sheet, LMS export) and completion status.
Session Catalogue	The forward programme: planned sessions with audience, objectives, frequency, delivery method, provider and — the part reviewers increasingly ask about — an effectiveness measure per session. This is the training-programme document that sits alongside the per-member records.
Jurisdiction Reference	How the training duty is quantified where you operate: the EU baseline, Germany's § 38 Abs. 3 BSIG with the ~4-hours-every-3-years benchmark from the explanatory materials, Latvia's regular-training rule with annual content review, Czechia's trained-governing-body duty, Belgium's CCB discretion model, Norway's Digital Security Act, and the UK's voluntary Cyber Governance Code of Practice.

The legal ladder

	The management bodies of essential and important entities must **approve** the Article 21 cybersecurity risk-management measures, **oversee** their implementation, and **can be held liable** for the entity's infringements of Article 21. Approval implies documented understanding — which is what the training duty exists to create.
	Members of the management bodies **are required to follow training**, so that they gain sufficient knowledge and skills to identify risks and assess cybersecurity risk-management practices and their impact on the entity's services. Employee training is *encouraged* here — the mandatory staff-training duty lives in Article 21(2)(g) instead, so track it separately.
	Germany's transposition, in force **6 December 2025** with no transition period: Geschäftsleiter must regularly attend training (Abs. 3) — a personal, non-delegable duty — and are personally liable for culpable breaches (Abs. 2), with recourse waivers by the company legally ineffective. The statute says only "regelmäßig"; the explanatory materials assume roughly a half-day (~4 hours) at least every three years as the benchmark.
	Supervisors sample **individual** records, not dashboards: name, role, date, duration, content mapped to the Article 20(2) objectives, provider, completion evidence, next due date — plus the programme document and the board minutes showing the trained body actually approving the Article 21 measure set.

How often is "regularly"? — national quantifications

Jurisdiction	Rule	Quantification
EU baseline	Art 20(2): members of management bodies required to follow training	None — purpose-defined only
Germany	§ 38 Abs. 3 BSIG: regular, personal, non-delegable; in force 6 Dec 2025	~4 h at least every 3 years (explanatory materials benchmark, not statute)
Latvia	Nacion■l■s kiberdroš■bas likums (1 Sep 2024) + Cabinet Reg. 397 (2 Jul 2025): management training required; regular staff training, content reviewed at least annually	Regular — commonly implemented as annual

Czechia	Act No. 264/2025 Coll. (1 Nov 2025): governing bodies must oversee cybersecurity and be properly trained	None fixed — keep documented evidence
Belgium	Law of 26 Apr 2024 Art 31 §2 + CCB guidance: regular training, entity's discretion on scope and duration	None — expectations higher for essential entities
Norway	Digitalsikkerhetsloven (in force 1 Oct 2025): management approves the security management system, annual review; training per NIS2 alignment	None fixed
UK	Cyber Security and Resilience Bill: no statutory training duty; voluntary Cyber Governance Code of Practice	None

The inspection-ready evidence pack

The log is one artefact in a five-piece pack supervisors converge on: **(1)** the named management-body register; **(2)** individual training records per member — this workbook; **(3)** the training-programme document — the Session Catalogue sheet; **(4)** board minutes showing the trained body approving the Article 21 measures (version, date, attendees by name); and **(5)** effectiveness evidence — tabletop reports, minuted briefings with follow-up actions, assessment results. Keep the evidence references in the log pointing at real stored artefacts: a certificate that cannot be produced on request does not exist, as far as an audit is concerned.

Why this matters now: Article 20 links training to liability. Management bodies that cannot evidence their own training while approving risk-management measures hand a supervisor an easy finding — and in Germany, § 38 Abs. 2 BSIG attaches personal, waiver-proof liability to exactly that gap. The log is the cheapest insurance in the NIS2 evidence stack.

> **From log to buyer-visible evidence.** The same governance evidence your supervisor samples is what enterprise buyers ask for in security questionnaires ("does management receive cybersecurity training?"). Orbiq publishes governance and training evidence in a governed Trust Center, so one record answers both. See orbiqhq.com/templates for the full free template library.