Security strategy: what goes on the one page that management signs?

Within six weeks, write a one-page strategy that ties three to five measurable security bets to the business plan, your crown jewels and a risk appetite in numbers, and have the management body approve it in a minuted decision. Review it every year before the budget, and sooner when an incident, acquisition, new law or new threat breaks one of its assumptions.

Reviewed	Next review	Version
5 Nov 2026	**5 Dec 2026**	**1.0**

Written for

Heads of security, CISOs and IT leads who own security, and the managing directors and boards who approve the strategy, especially in EU organizations with NIS2, BSIG or DORA duties

Latest version

sheets.einblick.dev/security-strategy/

If you only do five things

1. **Start from the business plan.** Read the company strategy and ask each business head what they plan for the next three years and what must not fail. The UK Cyber Governance Code asks boards for a cyber strategy aligned with, and embedded within, the wider organizational strategy[1].
2. **Name the crown jewels.** List the five to ten processes, data sets and systems whose loss would hurt most, each with a business owner. Have management agree the list, as the UK code's first risk action asks[1].
3. **Have management set the risk appetite.** NIST calls risk appetite the guidepost for setting strategy, set by the most senior leadership[2]. Write it in hours of downtime, euros and records exposed, not in colors. A small company can stop at downtime and data loss per crown jewel.
4. **Pick three to five bets you can measure.** Give each an outcome, a measure, a date and an owner, such as restoring the ERP within 72 hours in a test by the end of 2027. A product you plan to buy is not a bet.
5. **Get it approved, then review it yearly.** Under NIS2, the management body approves and oversees the security measures[3]. Minute the decision. Review the page at least yearly and after significant incidents or changes, the cycle Regulation 2024/2690 sets for digital providers' security policy[4].

Build it in six weeks

1. **Week 1: what do you already know?** Collect the business plan and budget, two years of incidents and near misses, the latest maturity assessment, audit and penetration test findings, customer and insurer demands, and the laws in scope from the EU security laws sheet. Book the management meeting for week 6 now.
2. **Week 2: what does the business need?** Interview the managing directors and six to ten heads of sales, operations, finance and product: what they plan, what can't stop for a day, what must never leak. NIST starts with the mission, goals and a business impact analysis[10].
3. **Week 3: what threatens the crown jewels?** Name the three or four likeliest attack paths from your incidents, your sector's warnings and ENISA's Threat Landscape, as the threat intelligence sheet describes. Draft the appetite and test it with the CFO.
4. **Week 4: which bets, and what do you drop?** Rank candidate initiatives by how much risk they take off the crown jewels per euro. Keep three to five and list the rest as later or won't do.
5. **Weeks 5 and 6: who signs?** Present the page with an annex of evidence and a budget range. Management approves it in a minuted decision, and the program sheet turns the bets into a roadmap.

What goes on the one page

- **Business goals.** Three to five goals from the company plan that security must support, such as winning a regulated customer or moving production to the cloud. Regulation 2024/2690 requires digital providers' security policy to fit the business strategy and objectives[4].
- **Crown jewels.** The processes, data and systems whose loss would stop the business or cost customer trust, each with an owner.
- **Threat picture.** The three or four attack paths most likely to reach them, one line each, with the evidence.
- **Risk appetite.** What management accepts, in numbers: for example, the web shop down at most 24 hours a year and no loss of payment data. NIST separates broad appetite from narrower tolerance: email available most of the day, but never down more than five minutes in core hours[2].
- **Three to five strategic bets.** Each with the outcome, a measure from the security metrics sheet, a date and an owner.
- **What you won't do.** Gaps you accept and things you buy rather than build, such as no in-house 24/7 SOC, so nobody keeps reopening them.
- **Dependencies and budget.** What the bets need from IT, suppliers, hiring and other projects, and a yearly budget range agreed with the CFO. The BSI lists a budget frame among management's risk criteria[8].
- **Approval and review.** The date the management body approved it, which 2024/2690 requires in digital providers' policy[4], and the next review date.

Who approves it

- **NIS2 entities.** The management body approves the risk management measures, oversees their implementation and can be held liable[3].

When to refresh it

- **Every year, before the budget.** Review the strategy's outcomes, as CSF 2.0 expects[9], and update the threat picture.

- **Germany.** Under BSIG § 38, management implements and oversees the § 30 measures and is liable to the entity for culpable damage[6]. The BSI says it can delegate implementation, not responsibility or oversight, and recommends resolutions as proof of involvement[8].
- **DORA.** The management body sets and approves the resilience strategy, including the ICT risk tolerance, and allocates the budget. Its ICT risk framework, strategy included, needs a yearly review[5].
- **Everyone else.** The managing directors sign it; unsigned, it moves no budget.

Mistakes that cost the most

- **A tool shopping list called a strategy.** Products say what you'll buy, not which risk goes down. Tools belong in the roadmap.
- **A compliance checklist as the strategy.** In ENISA's 2025 survey, 70% named regulatory compliance the main driver of their security investment[13]. Aim the bets at the crown jewels.
- **Fifteen priorities.** If everything is strategic, nothing is. Move the rest to the roadmap or the won't-do line.
- **An appetite without numbers.** "Low appetite for cyber risk" decides nothing until a tolerance in numbers says when it's exceeded.

What changed in 2026

- **German management duties apply.** BSIG § 38 has applied since 6 December 2025, with no general transition period[6,7].
- **The BSI listed the decisions to take.** Its October 2026 curriculum suggests, ideally within 2 to 6 weeks of the first training, approving a § 30 measures register with priorities, owners and budget needs, and rules for accepting risk[8]. Take them with the strategy.
- **Every three years, from scratch.** Redo the interviews and the crown jewels list.
- **When an assumption breaks.** An incident at you or a peer, an acquisition, a new law, critical supplier or threat. ENISA lists peer incidents, legal changes and threat trends among the inputs for reviewing digital providers' security policy[11].
- **Not for every headline.** Such events don't automatically require an update, ENISA notes; weigh them in the risk assessment first[11].

What you can skip

- **A 40-page strategy.** Nobody rereads it at the yearly review.
- **A security vision and mission.** Use the company's goals.
- **SWOT and trend workshops.** Incidents, the assessment and the interviews tell you more, faster.
- **Euro figures for every risk first.** Quantify only the close calls; see the risk register sheet.
- **A separate strategy per law.** Write one, with NIS2, DORA and customer demands as constraints.

- **NIST tied CSF to enterprise risk.** IR 8286 Rev. 1 (December 2025) lets you state appetite as permissible downtime, losses or a ceiling[2]; SP 1308 (March 2026) links profiles to risk and workforce decisions[10].
- **AI reaches more attack phases.** ENISA's 2026 Threat Landscape expects AI to directly enable more attack phases this year and still rates ransomware the most impactful short-term threat[12]. Recheck your threat picture.

What this looks like at your size

Small team, no security staff

- The managing director owns it; the IT provider helps draft it in two half-day sessions.
- Book the BSI's CyberRisikoCheck, ideally not from the provider that runs your IT: a 1 to 2 hour interview on 27 requirements, with a score and fixes by urgency[14].
- Three bets: a tested restore of email and files, phishing-resistant sign-in for admins and finance, exploited edge flaws patched within 72 hours.
- Won't do: hire security staff. Buy MDR.

Growing, with IT or security staff

- The head of IT or security drafts it, the management board approves it and a quarterly steering meeting tracks the bets.
- Show the gap with CSF 2.0 Current and Target Profiles[9], built from the maturity assessment.
- Agree a three-year budget range with the CFO and confirm it every year.
- Link each bet to rows in the risk register.

Enterprise or regulated

- Under DORA, the strategy must link ICT risk management to the business strategy and set ICT risk tolerance, KPIs and key risk metrics[5].
- Feed cyber risks into enterprise risk management and roll registers up to group level, as IR 8286 describes[2].
- Write one group strategy with an annex per regulated entity; each entity's management body approves its own.
- Have internal audit test delivery every year.

Version history

5 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which presented Regulation 2024/2690 and ENISA's review cycle as a benchmark for digital providers, not a duty for everyone, tied delegation limits to the BSI's curriculum and added DORA's yearly review of the strategy.

Sources

1. Cyber Governance Code of Practice. DSIT and NCSC, 8 Apr 2025. gov.uk
2. IR 8286 Rev. 1, Cybersecurity and ERM. NIST, Dec 2025. csrc.nist.gov
3. NIS2 Directive, Article 20. EUR-Lex, 2022. eur-lex.europa.eu
4. Regulation (EU) 2024/2690, Annex. EUR-Lex, 2024. eur-lex.europa.eu
5. DORA, Articles 5 and 6. EUR-Lex, 2022. eur-lex.europa.eu
6. BSIG § 38. BMJV, checked 5 Nov 2026. gesetze-im-internet.de
7. Fragen und Antworten zu NIS-2. BSI, checked 5 Nov 2026. bsi.bund.de
8. Curriculum für eine Geschäftsleitungsschulung nach NIS-2. BSI, 28 Oct 2026. bsi.bund.de
9. Cybersecurity Framework 2.0. NIST, 26 Feb 2024. nvlpubs.nist.gov
10. SP 1308, CSF 2.0 ERM Quick-Start Guide. NIST, Mar 2026. csrc.nist.gov
11. NIS2 Technical Implementation Guidance. ENISA, 26 Jun 2025. enisa.europa.eu
12. ENISA Threat Landscape 2026. ENISA, 22 Sep 2026. enisa.europa.eu
13. NIS Investments 2025. ENISA, 8 Dec 2025. enisa.europa.eu
14. CyberRisikoCheck. BSI, checked 5 Nov 2026. bsi.bund.de