Security program: what do you fund first, and how do you keep it on track?

This quarter, turn strategy bets and assessment gaps into 8 to 12 initiatives with an owner, outcome, cost and quarter each, rank them by risk reduction per euro after fixed deadlines, and get the roadmap and budget approved. Steer it monthly with the owners and quarterly with management, and change it only there.

Reviewed **5 Nov 2026** | Next review **5 Dec 2026** | Version **1.1**

Written for **Heads of security, CISOs and IT leads who own security, and the managing directors who fund the program**

Latest version **sheets.einblick.dev/security-program/**

If you only do five things

1. **Turn the gap list into a few initiatives.** Group bets, gaps, findings and risk rows into 8 to 12 initiatives, each with an owner, outcome, date and the requirements it meets[1].
2. **Rank by risk reduction per euro.** Weigh each one's cost against the risk it removes, as 2024/2690 requires of digital providers[2]. Count three years of cost. Then fund down the list until the money runs out, one of NIST's methods[3].
3. **Schedule fixed deadlines first.** Enter legal, audit and contract dates first, such as full CRA application on 11 December 2027 for product makers[4], then their prerequisites.
4. **Budget the run cost of every change.** Record one-time and recurring costs. The BSI warns that savings on technical measures often turn into high ongoing staff effort[5].
5. **Steer on a fixed cadence.** Track progress monthly, report to management at least quarterly[6] and change scope, order or budget only in those meetings.

Build the roadmap in four weeks

1. **Week 1: what goes in?** Collect the strategy sheet's bets, the maturity assessment's gaps, open audit and test findings, risk register rows above appetite, incident lessons and every legal or contract deadline.
2. **Week 2: which initiatives?** Merge measures that share a system or an owner; Grundschutz++ suggests weighing synergies between measures that meet several requirements[1]. Write one line each: outcome, owner, costs, dependencies.
3. **Week 3: what makes the cut?** Score each on risk reduction and three-year cost. NIST advises counting maintenance and operating labor, in the risk's own units[3]. Cut at the budget and show management the risk below the line[5].
4. **Week 4: who approves?** Order by deadline, dependency and capacity. Management approves, since it must provide the resources[1]. The security projects sheet delivers each initiative.

Budget size and structure

- **Benchmark, don't target.** In ENISA's survey of 1,080 mostly large EU organizations, security took a median 9% of the IT budget and 10.6% of IT staff[7]. Sector medians ran from 6% in energy to 13.3% in ICT service management[8].
- **A German survey finds more.** Bitkom's 2026 survey of firms with 10 or more staff found a mean of 18%, as in 2025; 45% spent 20% or more[9].
- **Count like ENISA.** Include capital and operating spend on hardware, software, staff, contractors and outsourcing[7].
- **Split run, change and reserve.** Run: staff, licenses, MDR, recurring tests. Change: initiatives with an end date. Reserve: about 10% of the money for incidents and findings.

Get it funded

- **Ask for outcomes, not products.** "ERP restored within 72 hours" survives a budget meeting; "a backup appliance" invites a cheaper quote.
- **Name the risk a no leaves.** NIS2 and the BSIG let implementation cost count, but measures must still fit the risk[10,11]. Have management record any no as its decision.
- **Attach the outside demand.** In ENISA's survey, 26% named customers' and 29% supply chain security requirements as investment drivers, only 7% executive or board requests[7].
- **Fund operators, not just tools.** Money is moving to technology and outsourcing, not internal teams[7]. Use what your licenses include, and retire an overlapping tool for each new one.

An 18-month roadmap, by half year

An example for a mid-size company: initiative, owner and the test that closes it.

Months 1 to 6

- **Phishing-resistant admin sign-in.** Head of IT. Done: every Tier 0 account uses a security key or passkey.
- **Timed ERP restore.** IT operations. Done: the test meets its recovery time objective.
- **One asset and supplier list.** IT and procurement. Done: every entry has an owner.

Months 7 to 12

- **EDR on every server.** IT operations. Done: every listed server reports in or has a dated exception.
- **MDR with planted tests.** Security. Done: a planted test is caught and escalated in time.
- **CRA readiness, for product makers.** Product security. Done: vulnerability handling and SBOMs by 11 December 2027[4].

Months 13 to 18

- **Management and backup zones.** Network team. Done: admin interfaces answer only from the admin subnet.
- **Critical supplier clauses.** Procurement. Done: the top-tier contracts carry them.
- **Reassess and replan.** Head of security. Done: the next roadmap is approved.

Steering cadence and the status page

- **Monthly working group, 60 minutes.** Owners, IT operations and security: status, blockers, small changes. Grundschutz++ wants escalation paths and no conflict of interest between implementer and tracker[1].
- **Quarterly management review.** Approve changes to scope, order and budget; accept the risk of each delay. The BSI suggests a regular report on risks, measures, incidents, suppliers, audits, maturity, budget and decisions[12].
- **Yearly replan before the budget.** Re-rank with the strategy review. Digital providers must review their risk treatment plan at least annually[2].
- **One status page.** A row per initiative: owner, outcome, due quarter, status in words, spend. Then blockers, changes, unplanned work and decisions. Outcomes go on the security metrics sheet's board page.

Close initiatives with evidence

- **Done means the outcome was tested.** "The restore ran in time", not "tool installed"; see the security projects sheet.
- **File the evidence.** Grundschutz++ asks for each measure's requirement, the date it was done or checked and who checked it, with evidence[1].
- **Hand over to run.** Name the operating owner, move the yearly cost into the run budget and add a metric.
- **Re-rate the risks.** The BSI expects management to hear of progress and the resulting risk reduction[5].
- **Compare plan with actuals.** Use the gap to correct the next estimates.

Mistakes that cost the most

- **Funding the project, not its operation.** The tool goes live and nobody has time to tune it.
- **Starting everything at once.** Cap the work in flight at what your owners can run.
- **Green until the last month.** Ask for the next milestone date, not a color or a percentage.
- **Reprioritizing in the corridor.** Changes outside the review reshuffle the plan after every incident.
- **Counting go-live as done.** Adoption decides whether the risk dropped.

Unplanned work and scope creep

- **Plan 70 to 80% of capacity.** Keep the rest for incidents, audits and customer questionnaires, and log the hours.
- **One intake for new work.** Small requests go to the working group; anything that moves a committed date waits for the quarterly review or a written management decision, and something else moves out. ENISA advises managing exceptions to the plan[13].
- **After an incident, replan.** Digital providers must feed post-incident reviews into risk treatment[2]. Re-rank at the next monthly meeting.
- **Give audit findings a date.** The BSI can make critical facility operators submit a plan to fix deficiencies their audits found[11].
- **Split off phase two.** Extra scope competes for funding as a new initiative.

What you can skip

- **Portfolio software.** A spreadsheet or the ticket system carries 8 to 12 initiatives; Grundschutz++ names a project or ticket system for owners and deadlines[1].
- **Detailed plans past six months.** Plan the rest by half year.
- **Exact ROI per initiative.** Quantify only the close calls; see the risk register sheet.
- **One program per law.** Run one roadmap and tag each initiative with the NIS2, DORA, CRA or ISO 27001 requirement it serves.

What changed in 2026

- **ENISA's newest data.** Its December 2025 report found spend steady at a median 9% of IT budgets but moving to tools and outsourcing, as security's share of IT staff hit a new low[7]. Budget operators too.
- **Grundschutz++ formalizes the plan.** BSI-Standard 300-1 (October 2026) wants a prioritized implementation plan with owners, deadlines and tracking, approved by management, which carries the risk of open items[1].
- **German critical facilities got resilience duties.** The KRITIS umbrella act took effect on 17 March 2026; its duties start 9 to 10 months after registration[14], which waits for its scope ordinance, still a draft[15]. Plan them on this roadmap.

What this looks like at your size

Small team, no security staff

- Keep one page of 3 to 5 initiatives with your IT provider and review it quarterly with the managing director.
- Have the provider price each one-time and monthly.
- Fund a tested restore and phishing-resistant admin sign-in before any new tool.

Growing, with IT or security staff

- Run 8 to 12 initiatives with a monthly working group and a quarterly management review.
- Keep the roadmap in a spreadsheet or the ticket system, linked to risk register rows.
- Hold back 20 to 30% of team capacity for unplanned work.

Enterprise or regulated

- Run one group roadmap; each regulated entity's management approves its part.
- Under DORA, minute the management body's budget allocation and reviews[16].
- Have internal audit sample closed initiatives every year.

Version history

5 Nov 2026, version 1.1 Confirmed that KRITIS registration still waits for the draft scope ordinance.

Sources

1. BSI-Standard 300-1, chapter 4. BSI, 20 Oct 2026. bsi.bund.de
2. Regulation 2024/2690, Annex. EUR-Lex, 2024. eur-lex.europa.eu
3. IR 8286B-upd1. NIST, Feb 2025. csrc.nist.gov
4. CRA, Article 71 and Annex I. EUR-Lex, 2024. eur-lex.europa.eu
5. BSI-Standard 200-2, chapter 9. BSI, Oct 2017. bsi.bund.de
6. Cyber Governance Code of Practice. DSIT and NCSC, 8 Apr 2025. gov.uk
7. NIS Investments 2025. ENISA, 8 Dec 2025. enisa.europa.eu
8. NIS Investments 2025, survey data. ENISA, Dec 2025. enisa.europa.eu
9. Wirtschaftsschutz 2026 (association survey). Bitkom, Sep 2026. bitkom.org
10. NIS2 Directive, Article 21. EUR-Lex, 2022. eur-lex.europa.eu
11. BSIG §§ 30 and 39. BMJV, checked 5 Nov 2026. gesetze-im-internet.de
12. Curriculum Geschäftsleitungsschulung. BSI, 28 Oct 2026. bsi.bund.de
13. NIS2 Implementation Guidance, 2.1. ENISA, 26 Jun 2025. enisa.europa.eu
14. KRITISDachG § 8. BMJV, checked 5 Nov 2026. gesetze-im-internet.de
15. FAQ zum KRITIS-Dachgesetz. BBK, checked 5 Nov 2026. bbk.bund.de
16. DORA, Article 5. EUR-Lex, 2022. eur-lex.europa.eu