First 90 days as head of security: what do you check, fix and decide?

In your first 30 days, find out who decides, which laws and promises bind you and whom to call, and fix five basics that need no strategy. Build the first risk register and a light maturity assessment in month two, and bring a strategy draft, operating model and first roadmap to management for approval by day 90.

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

Written for

New heads of security, CISOs and information security officers (ISBs), IT leads who take over security, and the managing directors they report to

Latest version

sheets.einblick.dev/first-90-days/

If you only do five things

1. **Get your mandate in writing.** In the first two weeks, have management confirm your role, reporting line, deputy and decision rights in a minuted decision; see the security team sheet. The BSI lists confirming the ISB or CISO reporting line among the decisions to take after management's first training[1].
2. **Listen for a month before you change anything.** Interview the managing directors and the heads of the business, IT, legal and data protection, and read what your predecessor left.
3. **Fix five basics without waiting for a strategy.** Admin MFA, backups, edge flaws, logging and the call chain can't wait. In ENISA's 2025 survey, patching (50%) and business continuity (49%) were the NIS2 areas organizations found hardest to implement[12].
4. **Measure in month two.** Write the first risk register rows and run a light maturity assessment, rating only what you saw working.
5. **Bring decisions to management by day 90.** Have a strategy draft, the operating model and a first roadmap with a budget approved in a minuted decision. Under NIS2, the management body approves the security measures and oversees their implementation[19].

Days 1 to 30: find out what you inherited

1. **Who decides?** List who approves budgets, accepts risks, signs exceptions and may shut down a system, and read two years of management minutes on security.
2. **Which laws and promises bind you?** Map each entity to NIS2, DORA and the CRA with the EU security laws sheet; in Germany, the BSI's anonymous NIS-2 check gives a first, non-binding answer[8]. Collect the security annexes and questionnaires sent to customers and insurers; see the customer assurance and cyber insurance sheets.
3. **Whom do you call?** Get three lists: admin accounts, Global and domain admins first; incident contacts, from the MDR to the insurer's hotline; suppliers with remote access. Regulation 2024/2690 requires digital providers to keep incident contact lists and supplier contact points[11].
4. **What went wrong before?** Read the last two or three years of incidents, near misses, audits and penetration tests, and check which findings were closed with evidence.
5. **Are the basics really in place?** Check the five fixes below yourself, on screen: a setting, a log entry, a restore record. A yes in a handover note isn't evidence.

Five fixes for month one that need no strategy

- **Phishing-resistant MFA for every admin.** Register security keys or passkeys, then require the Phishing-resistant MFA strength in Conditional Access (Entra ID P1 or Business Premium)[16] for at least Microsoft's 14 roles. Exclude break-glass accounts and start in report-only, or you can lock yourself out[15]. See the passkeys and MFA sheet.
- **One backup copy admins can't delete.** Give backups their own admin accounts and require MFA to change or delete them, as the NCSC advises[18]. Then time one restore, as the ransomware sheet describes.
- **No exploited flaw on an edge device.** Exploits opened 32% of Mandiant's 2025 intrusions[14]. Patch exploited firewall and VPN flaws in 72 hours, then run the edge devices sheet's compromise check.
- **Logging that is on.** Auditing isn't on by default in Microsoft 365 Business plans; check `Get-AdminAuditLogConfig`[17]. Without logs you may have to assume and disclose a worst-case data theft[14]. See the logging sheet.
- **A call chain that works at 3 a.m.** Name who is on call, who may shut systems down and who reports, each with a deputy, on paper. The BSI asks how the 24-hour deadline holds at night and on weekends[1]. See the incident response sheet.

German NIS2 entities: the BSIG duties to check first

- **Registration.** It's due within three months of falling in scope[3], and the BSI says the deadline has passed[5]. If you missed it, register in the BSI portal now with an ELSTER organization certificate from Mein Unternehmenskonto[5].
- **Current details.** The registration holds email, phone numbers and public IP ranges; report changes within two weeks[3]. Use a role mailbox the on-call person sees, since urgent BSI warnings may come at night[6].
- **Your own portal access.** Each user needs their own ELSTER certificate, activated by a letter that usually takes five working days or more. The BSI advises at least two owners; if the only one leaves, ask portal support[7].
- **The reporting chain.** Any employee given portal access may report, and a provider can be authorized to report for you, though responsibility stays with you[6]. The BSI starts the 24 hours when an employee learns of the incident during working hours[6]; the EU security laws sheet has the clocks.
- **Management training.** The managing directors must attend regularly[3]; training only the IT lead or ISB doesn't replace it[1]. Record provider, participants and roles, date, duration and content[2].

Days 31 to 90: measure, then decide

1. **Days 31 to 45: the first risk register rows.**
   Start from the asset list and the internet-facing systems the attack surface sheet finds. Write 20 to 30 risks with business owners, a first cut of the risk register sheet's 20 to 50, and reconfirm or expire inherited acceptances.
2. **Days 46 to 60: a light maturity assessment.**
   Compress the maturity sheet's five-week assessment into two: scope it to the crown jewels and sample one piece of evidence per outcome.
3. **Days 61 to 75: strategy draft and operating model.**
   Write the strategy sheet's one page and the operating model sheet's two pages; month one already covered the strategy's first two weeks.
4. **Days 76 to 90: first roadmap and approval.**
   Turn bets and gaps into the program sheet's 8 to 12 initiatives. German NIS2 entities can also approve the § 30 measures register the BSI suggests[1].

Reporting to management in the first 90 days

- **Day 30: what you found.** One page with the five basics and their status, what you fixed, the BSIG checks and the top five risks. Ask for one decision, such as funding the backup copy.
- **Day 60: risks and gaps.** The top ten risks and current against target per function, with no average score.
- **Day 90: the decisions.** Strategy, operating model, roadmap and budget. The BSI's list for management adds scope, governance, risk acceptance rules, the reporting process and a regular cyber risk report[1].
- **Minute every decision.** The BSI recommends resolutions, budget decisions and accepted residual risks as proof of management's active involvement[1]. Then switch to the security metrics sheet's quarterly page.

What you can skip in the first 90 days

- **New tools.** First list what your licenses include and what is switched off. Buy only what a quick fix needs, such as admin security keys.
- **Rewriting every policy.** Fix only rules that are dangerous or contradict the settings. The policies sheet's rewrite comes after the strategy.
- **Reorganizing on day 10.** You don't yet know who carries what. Move people after the operating model is approved.
- **A certification project.** Unless a contract sets a date, decide on ISO 27001 with the strategy; see the ISMS sheet.

Mistakes that cost the most

- **Believing the handover.** In ENISA's NIS360 2026, cloud and data center providers said they test incident plans regularly; their supervisors said oversight didn't show it[13].
- **Your predecessor's name on the call list.** Update the incident card, the BSI registration and the insurer and supplier contacts in week one.
- **Spending 90 days on tickets.** Block two days a week for interviews and planning, and hand routine work back to IT or the provider.
- **A strategy from your last job.** One written in week two describes the company you left. Write it after the interviews and the risk register.

What changed in 2026

- **German NIS2 duties apply.** By 30 September 2026, 20,141 entities had registered with the BSI under NIS2[9]. Check that yours is one.
- **The BSI published a model management training.** Its 28 October 2026 curriculum lists decisions to take ideally 2 to 6 weeks later[1].
- **Voice phishing became the second way in.** It opened 11% of Mandiant's 2025 intrusions, after exploits[14]. Check how the help desk verifies callers before an MFA reset; see the security awareness sheet.

What this looks like at your size

Small team, no security staff

- As IT lead or part-time ISB, start with the managing director and the IT provider.
- Have the provider show the five basics on screen and close the gaps in month one.
- Under 50 staff in Germany, make the maturity sheet's CyberRisikoCheck the light assessment.

Growing, with IT or security staff

- Interview 10 to 15 people in month one, including the works council and the data protection officer.
- Build the risk register and the CSF 2.0 profile with the IT team, not for it.
- Present strategy, operating model and roadmap in one management meeting.

Enterprise or regulated

- In week two, map each legal entity to its laws and supervisors. KRITIS umbrella act registration waits for its scope ordinance, still a draft[4].
- Read the last supervisory and internal audit findings before you set priorities.
- Each entity's management approves its own part.

Version history

5 Nov 2026, version 1.1 KRITIS registration now cites the BBK: it waits for the scope ordinance, still a draft.

Sources

1. Curriculum für eine Geschäftsleitungsschulung nach NIS-2. BSI, 28 Oct 2026. bsi.bund.de
2. Schulung für Geschäftsleitungen (Handreichung), version 1.0. BSI, 17 Apr 2026. bsi.bund.de
3. BSIG §§ 32, 33 and 38. BMJV, checked 5 Nov 2026. gesetze-im-internet.de
4. FAQ zum KRITIS-Dachgesetz. BBK, checked 5 Nov 2026. bbk.bund.de
5. NIS-2-regulierte Unternehmen. BSI, checked 5 Nov 2026. bsi.bund.de
6. NIS-2-Meldepflicht. BSI, checked 5 Nov 2026. bsi.bund.de
7. BSI-Portal FAQ. BSI, checked 5 Nov 2026. bsi.bund.de
8. NIS-2-Betroffenheitsprüfung. BSI, checked 5 Nov 2026. betroffenheitspruefung-nis-2.bsi.de
9. NIS-2 in Zahlen. BSI, as of 30 Sep 2026. bsi.bund.de
10. NIS2 Directive, Article 20. EUR-Lex, 2022. eur-lex.europa.eu
11. NIS2 technical implementation guidance, v1.0. ENISA, 26 Jun 2025. enisa.europa.eu
12. NIS Investments 2025. ENISA, 8 Dec 2025. enisa.europa.eu
13. ENISA NIS360 2026. ENISA, 28 May 2026. enisa.europa.eu
14. M-Trends 2026. Mandiant, Mar 2026. services.google.com
15. Phishing-resistant MFA for admin roles. Microsoft Learn, 24 Mar 2026. learn.microsoft.com
16. Conditional Access. Microsoft Learn, 27 Apr 2026. learn.microsoft.com
17. Turn auditing on or off. Microsoft Learn, 19 Jun 2026. learn.microsoft.com
18. Ransomware-resistant on premises backups. NCSC (UK), 22 Nov 2024. ncsc.gov.uk