Security team: who leads it, and whom do you hire next?

Within 30 days, have management appoint a head of security or information security officer (ISB) in writing, with a deputy and a direct line to the managing directors, outside IT operations. Then hire in the order your risks need, describe roles with ECSF profiles, and buy work that can't keep a person busy.

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

Written for

Managing directors, heads of security and IT leads who also own security, in small and mid-size companies and regulated organizations

Latest version

sheets.einblick.dev/security-team/

If you only do five things

1. **Appoint one owner in writing.** Have management appoint a head of security or ISB, a deputy and their authority in a minuted decision. ENISA counts appointments, job descriptions and proof of competence as evidence for digital providers[1].
2. **Give them a direct line to management.** Digital providers need at least one person reporting directly to the management body[2]. The BSI advises German NIS2 managers to confirm the ISB or CISO line early[3].
3. **Keep oversight out of IT operations.** The BSI advises against placing the ISB in the IT department[4]. Security engineering can sit in IT; the person who checks it shouldn't.
4. **Give every security role a deputy.** ENISA advises a deputy for each security role where possible[1]. Let the deputy run the monthly report while the lead is away.
5. **Hire for your top risk, buy the rest.** Buy what specialists do a few days a year: penetration tests, forensics, 24/7 monitoring. ENISA's 2025 respondents named finding skilled candidates as the top hiring barrier, at 45%[6].

Hire in this order

With the European Cybersecurity Skills Framework (ECSF) profile[10] and closest NICE work role[13]. Small companies stop after step 1 and buy the rest.

1. **Head of security or ISB.** ECSF Chief Information Security Officer, with information security officer as an alternative title; NICE Executive Cybersecurity Leadership. Owns strategy, policy, the ISMS and risk reporting.
2. **Security engineer.** ECSF Cybersecurity Implementer; NICE Systems Security Analysis. Owns identity, endpoint and cloud controls with IT.
3. **Detection and response lead.** ECSF Cyber Incident Responder; NICE Incident Response. Runs the MDR contract and incident plan. Detection and response topped ENISA's 2025 skills list[6].
4. **Risk and compliance.** ECSF Cybersecurity Risk Manager; NICE Cybersecurity Policy and Planning. Runs the risk register, regulatory evidence and customer questionnaires.
5. **Architect or deputy head.** ECSF Cybersecurity Architect; NICE Cybersecurity Architecture. Reviews project designs and deputizes for the head.

Where the head of security reports

- **Report to the CEO or managing director.** A CRO or COO also works if they don't run IT. In ENISA's 2021 survey, its latest to ask, 56% of heads of information security reported to the CEO or board, 29% to the CIO or an IT executive and 14% to risk management[9].
- **Under a CIO, write safeguards down.** The BSI sees an active admin as ISB as a likely conflict of interest[4]. Grant what the BSIG grants federal ISBs: a direct right to report to the top, and no removal or disadvantage for doing the job[15].
- **Separate admin work from oversight.** Digital providers must segregate conflicting duties; micro entities may compensate with management oversight or more logging[2]. A reviewer should be outside the line of authority under review[1]. The operating model sheet covers the three lines.

How big the team should be

- **About one in ten IT staff work on security.** The median share was 10.6% in ENISA's 2025 survey, the lowest yet[6], with a German median of 9.4%[7]. Most respondents were large organizations[6], so treat it as a cross-check, not a target.
- **Operations takes the largest share.** In ENISA's 2023 survey, operations held 40% of security staff, architecture and engineering 23%, governance and risk 21% and audit and compliance 16%[8].
- **Outsource operations, not governance.** 57% of those organizations used the most contractors in operations, only 9% in governance and risk; contractors were a median 20% of security staff[8].
- **Count the work, not the ratio.** List recurring tasks with hours per month, and make sure two trained people can do each one, in-house or at a provider.

ISB and data protection officer

- **The BSIG requires an ISB only of federal bodies.** With a deputy, independent reporting and protection from being penalized for the job[15]. Copy that into your ISB's appointment.
- **The ISB protects all information.** In the BSI's model, the ISB steers the security process, advises management and joins major projects, for paper as well as IT[4].

A virtual or fractional CISO

- **It fits part-time work.** Use one below about 250 staff, for a first ISMS or between hires. The BSI sees an external ISB as useful in small companies[4]; digital providers may give security roles to external parties[2].
- **Keep accountability and control in-house.** Responsibility and oversight can't be delegated, the BSI says[3]. Keep an internal coordinator, risk acceptance, the decision to report an incident, admin and emergency credentials, and the asset and supplier lists.

- **The DPO monitors data protection law.** They take no instructions on it, report to the top and may be external[16]. Germany requires one from 20 people regularly processing personal data by computer, or for processing that needs a DPIA.[17]
- **Keep the two apart.** Grundschutz++ calls DPO versus ISB a conflict to avoid[5]. The CJEU sees a possible conflict of interest when other duties have the DPO set the purposes and means of processing.[18]

Hiring and keeping security staff

- **Expect a skills gap.** In ISC2's survey, 59% had critical or significant skills needs, up from 44%[14]. ENISA found 94% of SMEs struggling to attract security staff.[6]
- **Test problem solving, not tool names.** Hiring managers in ISC2's survey ranked problem solving, teamwork and communication above any technical skill[14]. Use a work sample from your own environment.
- **Treat certificates as one filter.** Digital providers must check qualifications, for example by references, vetting, certifications or written tests[2]. ENISA lists certifications mapped to ECSF profiles.[12]
- **Fund training and the time for it.** In ENISA's 2023 survey, 47% had no specific security training budget[8]; in 2025, workload, training and career steps topped the retention problems.[6] Budget five protected days a year each.

What you can skip

- **A full-time CISO before there's a full-time job.** Below about 100 staff, let a part-time ISB with a deputy, an IT provider and MDR cover it.
- **An in-house 24/7 SOC.** A few analysts can't staff round-the-clock shifts. Buy MDR; see the SOC and MDR sheet.
- **One hire per ECSF profile.** The 12 profiles describe work, not headcount.
- **Certificates as the first filter.** Much of today's workforce came from other jobs through upskilling, ENISA notes[6]. Screen with a work sample.
- **Write the contract for the bad day.** Name the person and a deputy, hours per month, incident response time, deliverables, document ownership and exit handover. See the third-party risk sheet.
- **Don't hire your IT provider for it.** It would check its own work[1].

What changed in 2026

- **German duties apply.** Since 6 December 2025, BSIG § 38 has management implement and oversee the measures[15]. The BSI's new curriculum recommends confirming the ISB or CISO line within 2 to 6 weeks of the first training.[3]
- **Grundschutz++ names the conflicts.** BSI-Standard 300-1 of 20 October 2026 asks for roles with defined qualifications and no IT lead versus ISB or DPO versus ISB conflicts[5].
- **Germany plans to drop its national DPO rule.** On 4 December 2025, federal and state leaders agreed the federal government will propose repealing BDSG § 38(1) by the end of 2026[19]. It still applies.[17]
- **The role catalogs are moving.** NICE v2.2.0 added a supply chain risk role in April 2026[13]. ENISA plans to consult on a revised ECSF with proficiency levels at the end of 2026.[11] Map to the current 12 profiles now.

Mistakes that cost the most

- **Making the only admin the ISB.** They would judge their own work. If nobody else fits, buy an external ISB.
- **One person who knows everything.** When they leave, contacts, admin paths and open risks go too. Have the deputy work from the runbooks twice a year.
- **A title without time, budget or mandate.** Security roles need qualified people with enough resources, the BSI says[4]. Put hours, budget and decision rights in writing.

What this looks like at your size

Small team, no security staff

- Name an ISB with at least one day a week for the role, and a deputy. Not the only admin.
- If nobody fits, buy an external ISB and keep a managing director as the internal owner.
- Use an external DPO where you need one.

Growing, with IT or security staff

- Make the first full-time hire a head of security who reports to a managing director.
- Add a security engineer, then a detection and response lead who runs the MDR contract.
- Write job descriptions against ECSF profiles.

Enterprise or regulated

- Have the CISO report to the CEO or a board member who doesn't run IT.
- Under DORA, keep ICT risk control independent[20].
- German median in ENISA's 2025 survey: 19 security FTEs, contractors included[7].

Version history

5 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which labeled ENISA's guidance and Regulation 2024/2690 as applying to digital providers, confirmed ENISA's staffing medians and reporting-line data and narrowed the CJEU and BDSG points to what they say.

Sources

1. NIS2 Implementation Guidance. ENISA, 26 Jun 2025. enisa.europa.eu
2. Regulation (EU) 2024/2690, recitals 5 and 27, Annex 1.2 and 10. EUR-Lex, 17 Oct 2024. eur-lex.europa.eu
3. Curriculum für eine Geschäftsleitungsschulung nach NIS-2. BSI, 28 Oct 2026. bsi.bund.de
4. BSI-Standard 200-2, chapter 4. BSI, 2017. bsi.bund.de
5. BSI-Standard 300-1, v1.0. BSI, 20 Oct 2026. bsi.bund.de
6. NIS Investments 2025. ENISA, 8 Dec 2025. enisa.europa.eu
7. NIS Investments 2025, survey data. ENISA, Dec 2025. enisa.europa.eu
8. NIS Investments 2023. ENISA, 16 Nov 2023. enisa.europa.eu
9. NIS Investments 2021. ENISA, 17 Nov 2021. enisa.europa.eu
10. ECSF Role Profiles. ENISA, 19 Sep 2022. enisa.europa.eu
11. European Cybersecurity Skills Framework. ENISA, checked 5 Nov 2026. enisa.europa.eu
12. Certifications mapped to the ECSF. ENISA, checked 5 Nov 2026. enisa.europa.eu
13. NICE Framework Components v2.2.0. NIST, 28 Apr 2026. nist.gov
14. 2025 ISC2 Cybersecurity Workforce Study (association survey). ISC2, 4 Dec 2025. isc2.org
15. BSIG §§ 38 and 45. BMJV, checked 5 Nov 2026. gesetze-im-internet.de
16. GDPR, Articles 37 to 39. EUR-Lex, 2016. eur-lex.europa.eu
17. BDSG § 38. BMJV, checked 5 Nov 2026. gesetze-im-internet.de
18. Judgment C-453/21 (X-FAB). CJEU, 9 Feb 2023. eur-lex.europa.eu
19. Föderale Modernisierungsagenda, ch. 2, III.2.2. Bundeskanzler and Länder, 4 Dec 2025. rlp.de
20. DORA, Article 6(4). EUR-Lex, 2022. eur-lex.europa.eu