Operating model: who decides, who does it, who checks?

This quarter, write down on two pages who decides, who does the work and who checks it for six core processes, from patching to exceptions, and have management approve it. Buy the work wherever that is cheaper, but keep decisions, risk acceptance and supplier oversight with your own named people.

Reviewed	Next review	Version	Written for
5 Nov 2026	**5 Dec 2026**	**1.0**	**Heads of security and CISOs, IT leads who own security, and the managing directors they report to**

Latest version
sheets.einblick.dev/operating-model/

If you only do five things

1. **Give each core process one accountable name.**
   Name one A and the people who do the work for each of the six processes below. NIST suggests documenting who is responsible, accountable, consulted and informed[1].
2. **Write down who decides what.**
   The BSI's training curriculum asks management which cyber decisions need its approval[2]. Then list who accepts which risk and approves which exception.
3. **Separate doing from checking.**
   Assurance isn't credible if the reviewer designs or operates the process, the IIA says[3]. Don't let those who run systems audit them.
4. **Buy the work, keep the decisions.**
   NIS2 leaves approving and overseeing the measures with management[16], and the BSI says outsourcing all IT doesn't move the responsibility[4].
5. **Get it approved and review it yearly.**
   For digital providers, Regulation 2024/2690 has management review roles at planned intervals and after significant incidents or changes[5]. Do the same yearly and after every reorganization.

Write it down in two pages

1. **Page 1, top: scope and structure.**
   Entities, sites and main suppliers in scope, who leads security, and whether it runs central, federated or hybrid.
2. **Page 1, below: RACI and three lines.**
   One row per core process with one A each, then who operates, who monitors and who checks independently.
3. **Page 2, top: the service catalog.**
   Each service, such as project reviews, exceptions, scanning, supplier checks, incident response and audit evidence, with how to ask, how fast (project reviews within 5 working days, say) and who delivers it. Add what security doesn't do: patch, grant access, sign contracts.
4. **Page 2, middle: the decision table.**
   Who accepts which risk, approves which exception and may stop which system, each with a deputy.
5. **Page 2, bottom: approval.**
   The phone chain, the next review date and management's sign-off. ENISA advises dating the organization chart and naming who updated it[6].

A RACI for six core processes

A answers for the outcome, R does the work, C is asked before and I is told after. Keep one A per row. ENISA maps the roles requirement of 2024/2690 to ISO/IEC 27001 clause 5.3[6], so one RACI can serve both.

- **Patching.** A: head of IT. R: IT operations or the MSP. C: security, which sets deadlines from the patching sheet, and system owners for maintenance windows. I: management, about exploited flaws past deadline.
- **Vulnerability management.** A: head of security. R: security scans, rates and tracks; system owners fix. C: IT operations. I: management, monthly. Digital providers must document why a finding needs no fix[5].
- **Access reviews.** A: each application's business owner. R: the owner's team leads, with lists from IT. C: security, for admin rights. I: internal audit. Digital providers must document results and changes[5].
- **Incident response.** A: head of security. R: the SOC or MDR and IT operations. C: legal, data protection, communications. I: management and insurer; a named owner files reports to authorities (EU security laws sheet). Stopping business processes is for the crisis team.
- **Supplier onboarding.** A: the business owner who wants the supplier. R: procurement, with a contract manager per contract[7]. C: security, for tier and clauses. I: IT, to grant and later remove access.
- **Exceptions.** A: the risk owner, at the level set in the risk register sheet. R: the requester, with the case, a compensating measure and an end date. C: security. I: management, via the open exceptions list.

Three lines, applied to security

- **First line: whoever runs it.** The IIA's first line owns the risk and runs the controls[3]: IT operations, the MSP, application owners.
- **Second line: security.** It advises, monitors and challenges the first line[3]. If it also runs the firewall or EDR, have someone else check that.
- **Third line: someone independent.** Internal audit, in-house or bought in. The IIA treats at least 12 months between running and assuring a process as typically enough for objectivity[3].
- **Small companies may merge the first two.** The rules for digital providers allow duties on top of existing roles and, where size rules out reviewers outside the reviewed line, other ways to keep reviews impartial[5].

Central, federated or hybrid

- **Central.** One team sets the rules and runs security for everyone. Choose it when one IT team runs everything.
- **Hybrid.** Central security owns the standards, risk register, MDR and scanning; units patch, review access and name champions. Choose it for most growing companies.
- **Federated.** Each unit has its own security officer, as the BSI describes for large organizations[9]. Choose it for subsidiaries with their own IT and, where in scope, their own duties under the BSIG[10], and keep one shared risk register.

What to buy and what to keep

- **Buy what is rare or round the clock.** The NCSC says a SOC can outsource seldom-used functions, though in-house staff know the business better[11]. Typical buys: MDR (see the SOC and MDR sheet), pentests, a response retainer, a virtual CISO.
- **Put a responsibility matrix in the MSP contract.** State what the MSP does and what stays with you, as the NCSC advises[12].
- **Know which line a provider is in.** The IIA places providers in the line of whoever engages and directs them[3]: a pentest ordered by IT isn't independent.
- **Keep risk acceptance and supplier oversight.** DORA makes financial entities above micro size name a role to monitor ICT suppliers[13]. Give every supplier an internal owner anyway.

Security champions in business and IT teams

- **Name one per team that holds risk.** IT operations, development, finance for payment changes, HR for leavers and plant operations for OT.
- **Put their time in writing.** OWASP advises formally allocating champions' time and getting management support, because formal priorities win when priorities conflict[15].
- **Give them tasks, not authority.** They triage findings, review risky changes and are first contact in incidents, but don't approve exceptions.

What you can skip

- **A RACI for every task.** Six processes and a decision table settle most disputes. Add a row only when a dispute comes back.
- **An internal audit department in a small company.** Buy a yearly review from an auditor who neither runs nor advises on your IT.
- **A target operating model deck.** Two pages people use beat 40 slides nobody opens.

Decision rights and escalation

- **Let delegates accept smaller risks.** 2024/2690 lets digital providers delegate to accountable people with the authority, if management gets adequate reports[5]. Set levels with the risk register sheet.
- **Pre-authorize containment.** Let on-call staff or the MDR isolate a device or disable an account without asking. Leave business shutdowns to the crisis team.
- **Escalate on triggers.** IIA auditors must check for a process that escalates unacceptable cyber risks quickly[8]. Set triggers such as an exploited flaw past its deadline.
- **Set when security must be asked.** Grundschutz++ requires defining when the security officer joins projects[14].

What changed in 2026

- **The IIA updated its Three Lines Model.** Its July 2026 Statement of Position adds guidance for organizations not required to keep separate assurance functions[3]. Recheck where you've merged lines.
- **Internal audit now checks roles.** Since 5 February 2026, cyber audits must assess roles and escalation[8]; since 15 September 2026, supplier audits must assess who selects, manages and monitors suppliers[7].
- **The BSI spelled out delegation limits.** Its non-binding October 2026 curriculum on BSIG § 38 says management may delegate operational work, not responsibility or oversight, and suggests a responsibility matrix[2].

Mistakes that cost the most

- **Two accountable people for one process.** Then nobody is. Split the process or pick one.
- **Security as A for everything.** IT and the business then stop treating patching and access as their job.
- **No deputies.** ENISA advises a deputy for each security role where possible[6]. Name one for every A and test the phone chain twice a year.

What this looks like at your size

Small team, no security staff

- The managing director accepts risks; the IT lead or MSP runs the controls.
- Write the two pages with your MSP and approve them in a management meeting.
- Merge the first two lines if you must, but buy the independent check.

Growing, with IT or security staff

- Run hybrid, with champions in IT and business teams.
- Don't make the IT lead the security officer: Grundschutz++ calls that a conflict to avoid[14].
- Publish the service catalog and the decision table.

Enterprise or regulated

- Name security officers per unit or entity, under one group standard and register.
- Keep an assurance map of who checks which risk, to find gaps and duplicates[3].
- Under DORA, keep ICT risk control separate from internal audit[13].

Version history

5 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which labeled every Regulation 2024/2690 rule as applying to digital providers, quoted the IIA's July 2026 position on the three lines exactly and narrowed the NCSC sourcing advice to SOCs.

Sources

1. CSF 2.0 Implementation Examples, GV.RR-02. NIST, 26 Feb 2024. nist.gov
2. Curriculum für eine Geschäftsleitungsschulung nach NIS-2. BSI, 28 Oct 2026. bsi.bund.de
3. Statement of Position: Three Lines Model. IIA, 8 Jul 2026. theiia.org
4. Fragen und Antworten zu NIS-2. BSI, checked 5 Nov 2026. bsi.bund.de
5. Implementing Regulation (EU) 2024/2690, Annex. EUR-Lex, 17 Oct 2024. eur-lex.europa.eu
6. NIS2 technical implementation guidance and mapping table v1.2. ENISA, 26 Jun 2025. enisa.europa.eu
7. Third-Party Topical Requirement. IIA, effective 15 Sep 2026. theiia.org
8. Cybersecurity Topical Requirement. IIA, effective 5 Feb 2026. theiia.org
9. BSI-Standard 200-2, chapter 4. BSI, Oct 2017. bsi.bund.de
10. BSI-Gesetz (BSIG), § 38. BMJV (Germany), checked 5 Nov 2026. gesetze-im-internet.de
11. Building a SOC: Designing an operating model. NCSC (UK), 23 May 2022. ncsc.gov.uk
12. Choosing a managed service provider. NCSC (UK), 24 Nov 2025. ncsc.gov.uk
13. Regulation (EU) 2022/2554 (DORA), Art. 5 and 6. EUR-Lex, 2022. eur-lex.europa.eu
14. BSI-Standard 300-1, version 1.0. BSI, 20 Oct 2026. bsi.bund.de
15. Security Champions Guide. OWASP, checked 5 Nov 2026. securitychampions.owasp.org
16. Directive (EU) 2022/2555 (NIS2), Art. 20. EUR-Lex, 2022. eur-lex.europa.eu