Maturity assessments: where does your security really stand, and where should it be?

This quarter, pick one model that fits your company and run a five-week assessment that rates each outcome only on evidence you sampled. Set a target per function from your risks, not the top level everywhere, and show management gaps and decisions, not one maturity number.

Reviewed	Next review	Version	Written for
5 Nov 2026	**5 Dec 2026**	**1.1**	**Heads of security, CISOs, IT leads who own security, and the managing directors they report to**

Latest version
sheets.einblick.dev/maturity-assessment/

If you only do five things

1. **Pick one model and keep it.**
   Use the model your regulator or sector expects; otherwise NIST CSF 2.0 Profiles with the CIS Controls underneath. Keep the model, scale and scope from year to year, so results compare.
2. **Scope by business service.**
   Assess the services the company can't do without, with their cloud tenants, OT, suppliers and subsidiaries. A CSF Profile can cover the whole organization or one part, such as the financial systems[1].
3. **Rate only what you saw working.**
   Interview the people who run each control, then check a sample: settings, tickets, a restore record. NIST's assessment methods are examine, interview and test[4]. No evidence means not achieved.
4. **Set a target per function.**
   Decide where each function must be from your risks and duties. NIST encourages higher Tiers when risks or mandates are greater or a cost-benefit analysis supports it[1].
5. **Report gaps and decisions, not a score.**
   Show current against target per function, the gaps that matter and what you need decided. A "level 3" is a set of qualities, not a numerical value, as NIST notes[5].

Choose a model by company type

1. **Do you run UK essential services?**
   Use the NCSC CAF v4.0: 41 outcomes, judged achieved, partially achieved or not achieved[6], against the cross-sector Core Profile[8].
2. **Do you run energy or OT?**
   Use C2M2 v2.1: 356 practices in 10 domains, for IT and OT. DOE's tools are free to any organization, and its self-evaluation is designed to cover one function in a day[9].
3. **A German company under 50 staff?**
   Book a CyberRisikoCheck (DIN SPEC 27076): an IT service provider checks 27 requirements in a 1 to 2 hour interview and reports a score and ranked recommendations[18]. It rests on your answers, so ask for spot checks.
4. **Is your ISMS built on IT-Grundschutz?**
   Use the IT-Grundschutz-Check: interviews plus spot checks against each requirement[15]. Grundschutz++ marks each requirement met, not met or not applicable, with evidence[16].
5. **Everyone else?**
   Build CSF 2.0 Current and Target Profiles in NIST's free template[2], with CIS Controls as the checklist: IG1's 56 safeguards for small firms, IG2's 74 more once you have IT staff and sensitive data[11].

Run one in five weeks

1. **Week 1: what's in scope, and who answers?**
   List services, sites, tenants, OT and suppliers, in the fewest assessments that still give an accurate picture[9]. Name one contact per area[15].
2. **Weeks 2 and 3: interviews and samples.**
   Interview in pairs, one asking and one taking notes[15]. For each outcome, collect one record and check one live sample.
3. **Week 4: calibrate and set targets.**
   Review the ratings with the interviewees[9] and one person outside the control's team. Agree targets with management.
4. **Week 5: report and hand over.**
   Present gaps and decisions; the security program sheet turns gaps into a roadmap.

Evidence over self-scoring

- **Write the rule first.** In the CAF, one "not achieved" indicator normally decides the rating; "achieved" normally needs every achieved indicator[6].
- **Sample, don't ask.** Check five leavers' accounts, three servers' patch levels and the last restore record. The BSI suggests checking interview answers against documents, sites and system settings[15].
- **Record each rating's source.** Grundschutz++ assigns evidence to each measure and, for automated checks, records tool, time and result[16].
- **Count coverage where you can.** CIS's Assessment Specification defines measures and metrics per safeguard, such as how many endpoints implement it[12].

Current and target profiles

- **One row per outcome.** NIST's template has columns for practices, status, rating, priority and goals[2]. Add evidence and an owner.
- **Targets per function.** Set Tiers overall or per Function or Category, not per Subcategory[3]. Tiers rate the rigor of risk governance and management[1]; per-outcome ratings show whether practices work.
- **A floor everywhere.** C2M2 is built so every company can reach MIL1 in all domains[9]. For US critical infrastructure, CISA's CPG 2.0 sets a foundational level[10]. Go higher where your risks need it.

Presenting results to management

- **No average.** An overall 2.7 hides a zero in Recover. Show current and target side by side for each function.
- **Say how you know.** Name the model version, profile and scope, whether it was self-assessed or independently reviewed, and its limits, as the NCSC asks for CAF results[7].
- **Tie each top gap to a risk.** Give its entry in the risk register (see the risk register sheet), the cost to close it and your recommendation.

- **Reassess every 12 months** and, as DOE advises, after major business, technology or threat changes[9]. NIS2 entities in Germany need policies and procedures to assess their measures' effectiveness (BSIG § 30(2) no. 6).[20].

External assessor or your own team

- **Run the yearly cycle yourself.** Your people know where the evidence is; C2M2 is built for facilitated self-evaluation[9].
- **Buy independence where it counts.** Independent audit or testing generally gives more confidence, the NCSC says[7]. Use it every 2 to 3 years and when customers or regulators rely on the result, never from the firm selling the fixes.
- **Keep reviewers out of the line.** Under 2024/2690, digital providers need reviewers with audit competence; staff reviewers must sit outside the reviewed area's line of authority[19]. Others can copy the rule.
- **Check the licenses.** The CIS Controls are free for any company improving its own security; a consultant who assesses you with them or CSAT needs a CIS commercial license, such as SecureSuite membership[13,14].

What you can skip

- **A second framework for comparison.** Map once through informative references to ISO/IEC 27001 or SP 800-53[2].
- **Tiers for every Subcategory.** NIST says Function or Category level gives a better picture[3].
- **Peer benchmark scores.** Ratings from different assessors, scopes and scales don't compare. Compare yourself with last year.
- **A maturity platform before the first cycle.** NIST's spreadsheet template and your ticket system will do[2].

- **Ask for a decision.** Fund it, accept it with an end date where the law allows, or defer it. Track it on the security metrics sheet's quarterly page.
- **Show what moved.** Next year, show what changed and why, on the same scale.

What changed in 2026

- **The UK set a cross-sector CAF minimum.** The NCSC's Core Profile, published 30 October 2026, sets the expected level for each CAF v4.0 outcome against moderately sophisticated attackers[8].
- **Grundschutz++ drops "partially".** BSI-Standard 300-1, dated 20 October 2026, marks each requirement met, not met or not applicable[16]; the IT-Grundschutz-Check also allowed partially[15]. The BSI plans performance indicators for the method's requirements by 31 March 2027.[17].

Mistakes that cost the most

- **Scoring the paper.** The BSI rates "yes" only for measures implemented fully, effectively and appropriately[15], not for a signed policy.
- **Chasing the top level everywhere.** MIL3 or Tier 4 costs most where risk is lowest; DOE calls the top MIL in all domains not typically optimal[9].
- **Buying a score.** Tools that turn questionnaires or external scans into a maturity number measure answers or the perimeter, not practice.
- **Taking "implemented" for "works".** CIS's specification checks only whether a safeguard is implemented[12]. Test a restore or an alert.
- **Changing the yardstick.** A new model, scale or scope breaks the trend.

What this looks like at your size

Small team, no security staff

- In Germany, book a CyberRisikoCheck[18] yearly, ideally not from the provider that runs your IT.
- Elsewhere, rate yourself against CIS IG1 with one piece of evidence per safeguard.
- Take the managing directors through the top five gaps in one hour.

Growing, with IT or security staff

- Build Current and Target Profiles per CSF Function in NIST's template, with CIS IG2 as the checklist.
- Have someone outside IT operations, such as internal audit, recheck a sample.
- Finish the assessment before budget planning.

Enterprise or regulated

- Use the model your regulator expects, such as the CAF Core Profile for UK essential services. In energy and OT, use C2M2.
- Assess each subsidiary or business unit with the same scale and evidence rules.
- Report independent reviews to management, as 2024/2690 requires of digital providers[19].

Version history

5 Nov 2026, version 1.1 Added CISA's Cybersecurity Performance Goals 2.0 as the foundational level for US critical infrastructure.

Sources

1. Cybersecurity Framework (CSF) 2.0. NIST, 26 Feb 2024. nvlpubs.nist.gov
2. SP 1301, Organizational Profiles guide. NIST, Feb 2024. nvlpubs.nist.gov
3. SP 1302, CSF Tiers quick-start guide. NIST, Oct 2024. nvlpubs.nist.gov
4. SP 800-53A Rev. 5. NIST, updated 27 Aug 2025. csrc.nist.gov
5. SP 800-55v1, Measurement Guide. NIST, Dec 2024. csrc.nist.gov
6. Cyber Assessment Framework 4.0. NCSC (UK), Aug 2025. ncsc.gov.uk
7. CAF overview. NCSC (UK), reviewed 30 Oct 2026. ncsc.gov.uk
8. CAF Core Profile. NCSC (UK), 30 Oct 2026. ncsc.gov.uk
9. C2M2 Version 2.1. US DOE, Jun 2022. energy.gov
10. Cybersecurity Performance Goals 2.0. CISA, Dec 2025. content.govdelivery.com
11. Implementation Group 2. CIS, checked 5 Nov 2026. cisecurity.org
12. Assessment Specification v8.1. CIS, checked 5 Nov 2026. cas.docs.cisecurity.org
13. CIS Critical Security Controls FAQ. CIS, checked 5 Nov 2026. cisecurity.org
14. CIS CSAT terms of use. CIS, checked 5 Nov 2026. csat.cisecurity.org
15. BSI-Standard 200-2. BSI, Oct 2017. bsi.bund.de
16. BSI-Standard 300-1, v1.0. BSI, 20 Oct 2026. bsi.bund.de
17. Grundschutz++ milestone plan. BSI, Oct 2026. bsi.bund.de
18. CyberRisikoCheck. BSI, checked 5 Nov 2026. bsi.bund.de
19. Regulation (EU) 2024/2690. EUR-Lex, 17 Oct 2024. eur-lex.europa.eu
20. BSIG § 30. BMJV (Germany), checked 5 Nov 2026. gesetze-im-internet.de