Risk register: who may accept which risk, and for how long?

This quarter, build a register of 20 to 50 risks, each tied to a service on your asset list and owned by a business owner, and have management approve who may accept which risk and for how long. Review the top ten with management every quarter, and give every accepted risk and policy exception an end date no more than 12 months out.

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

Written for

Heads of security, CISOs and IT leads who keep the risk register, and the managing directors and business owners who accept risks, especially in EU organizations with NIS2, BSIG or DORA duties

Latest version

sheets.einblick.dev/risk-register/

If you only do five things

1. **Keep dozens of risks, not hundreds.**
   Write one row per scenario management would act on; aim for 20 to 50. NIST lets you set a minimum exposure for the register, since many low risks need no row[1].
2. **Tie each row to the asset list.**
   Use the service or asset ID from your inventory, so a new or retired system shows which risks change. ENISA's NIS2 guidance has the treatment plan link each risk to its assets and measures[10].
3. **Give every risk a business owner.**
   Grundschutz++ makes the business process owner the risk owner unless you decide otherwise[5]. IT runs the controls; it can't decide how long sales may be down.
4. **Write down who may accept what, until when.**
   Tie authority to impact, require reasons in writing and set an end date. Grundschutz++ requires a time limit on every temporary acceptance[5].
5. **Review the top ten every quarter.**
   Show management the status, slipped dates and expiring acceptances, and ask for decisions. The BSI's sample curriculum for management training lists a top-10 risk list with measure status[6].

Fill in one row

The isms sheet covers the ISO 27001 risk process around this register; the strategy sheet sets the risk appetite behind your scales.

1. **Which service or asset?**
   Name the business process or service and its ID on the asset list. Grundschutz++ identifies risks per process and adds single critical assets only where the process view misses them[5].
2. **What could happen?**
   Write a scenario: threat source, event, weakness, asset and harm, the elements NIST names[1]. For example: ransomware through the unpatched VPN encrypts the ERP and stops shipping for five days.
3. **What protects it today?**
   List the controls in place and planned, with their status, as Grundschutz++ requires[5]. Count only controls you have seen work, as the maturity sheet advises.
4. **How likely, and how bad?**
   Rate both on the scales below for today's state. NIST rates current, not inherent, risk, since some measures are typically in place[1].
5. **Who owns it?**
   Name a person with the budget and authority to act. NIST suggests the business owner, such as a business unit's general manager[3].
6. **What will you do, and by when?**
   Reduce, avoid, transfer or accept. Link the measures by ticket and set a due date and a review date. Insurance shifts some of the cost, not lost customer trust[1]; see the cyber insurance sheet.

Scales that two people score the same

- **Use four levels, defined in numbers.** The BSI's likelihood bands: at most once in five years, up to once a year, up to once a month, several times a month[4]. Our impact bands at €50 million revenue: under €50,000, up to €500,000, up to €5 million, above.
- **Leave out the middle.** The BSI advises at most five levels, and says two staff rating one risk should get the same result[4]. Four levels force a choice; test them on three sample risks.
- **Quantify the close calls.** When a decision hinges on whether a €300,000 measure pays off, estimate the yearly loss as a range. NIST describes three-point estimates, calibration and Monte Carlo simulation[2].
- **Use FAIR where euros decide.** The Open Group's FAIR standards are O-RA 2.1 and O-RT 3.1 (May 2025)[12]. Agencies told NIST calibrated frequency ranges can improve the yearly loss estimate[2].

Who may accept which risk

- **Acceptance is the exception.** NIS2 requires measures appropriate to the risks[8]; 2024/2690's recitals keep acceptance for exceptional cases[9]. The BSI rules out blanket acceptance under the BSIG, but risks irrelevant to the regulated services may be accepted[7].
- **Set authority by impact.** Our ladder: low risks the risk owner, medium a managing director, high and very high the management body. 2024/2690 lets digital providers delegate if management gets adequate reports[9]. Grundschutz++ has management authorize all residual risks[5], so add delegated ones to its quarterly sign-off.
- **Get it in writing, with reasons.** Digital providers must document the reasons[9]; ENISA adds a loss estimate and a contingency plan[10].
- **Give it an end date,** 12 months at most. DORA's full framework has accepted residual risks listed with reasons and reviewed at least yearly[11].
- **Don't accept critical flaws.** ENISA advises against it where possible[10]. Without a patch, digital providers must add measures and accept the residual risk[9].

Policy exceptions

- **Treat an exception as a small acceptance,** with the same authority levels. Record clause, systems, reason, compensating controls, end date and approver in one ticket form linked to the register row. ENISA lists request and approval records with compensating controls as evidence[10].
- **Demand controls that serve the rule's purpose.** ENISA's example is a system that can't support MFA, excepted while alternative measures go in[10]. Our choice: a jump host with MFA, a fixed source network and alerts.
- **End it, or approve it again one level up.** Grant up to 6 months, 12 at most. A renewal needs fresh approval and proof the compensating controls run.
- **Fix rules that collect exceptions.** Change the standard; see the policies sheet. Grundschutz++ allows no exception to a MUSS requirement; many permanently unmet SOLLTE ones can mean missing the state of the art[5].

Review cadence and reporting

- **Monthly: owners and security.** Update measure status, chase overdue dates and flag acceptances and exceptions expiring within 60 days. NIST suggests checking periodically, such as monthly, that each owner still fits[3].
- **Quarterly: the top ten to management.** Per risk: criticality, measure, owner, deadline and residual risk, as in the BSI's model dashboard[6]. Add expiring acceptances, open exceptions per policy and the decisions needed; the security metrics sheet sets the board page.
- **Yearly: the whole register.** Re-rate every row and archive what no longer applies, as NIST suggests[1]. Digital providers must review at least annually and after significant changes or incidents[9].
- **After each significant incident or near miss.** Check whether the register held the scenario and rated it right, and link the incident ticket to the row. ENISA lists post-incident findings among the review inputs[10].

What changed in 2026

- **Grundschutz++ set minimum register fields.** BSI-Standard 300-1 (20 October 2026) requires ID, object, description, protection goals, risk level and owner per risk, priority, treatment and linked measures where treated, and a time limit on temporary acceptance[5].
- **The BSI listed management's decisions.** Its non-binding curriculum suggests settling accepted risks, escalation thresholds and acceptance rules, ideally 2 to 6 weeks after the first training[6].
- **NIST revised its register series.** IR 8286, 8286A and 8286C Rev. 1 came out in December 2025[2,3]. IR 8286 encourages stating risk in money wherever feasible[1].

What you can skip

- **A row per threat catalog entry.** The BSI's 47 elementary threats[5] help find scenarios; copied per asset, they bury the ten that matter.
- **Inherent risk scores.** A world without controls is guesswork. Rate today's state and the target.
- **FAIR for every row.** Quantify the three to five close decisions; the four-level scale serves the rest.
- **A separate exceptions database.** Keep exceptions as tickets linked to register rows, with the end date as the due date.

Mistakes that cost the most

- **A register nobody reads.** Two hundred rows only the auditor sees decide nothing. Take the top ten to management and ask for a decision on each.
- **Every risk rated medium.** Scores bunch up; the BSI notes most users tend to use just two levels[4]. Define four in numbers; let an outsider challenge ratings.
- **IT owning business risks.** IT then accepts outages it can't weigh against revenue. Make the process owner the risk owner and IT the action owner.
- **Accepting by silence.** A risk nobody decides on is accepted by default. Put every undecided row on the next management agenda.
- **Exceptions without end dates.** They quietly become the policy. Alert 30 days before expiry and treat an expired exception as a finding.

What this looks like at your size

Small team, no security staff

- Keep 15 to 25 rows in a spreadsheet; the IT provider drafts, department heads own.
- A managing director accepts anything above low, in writing.
- Review it with the managing directors for 30 minutes a quarter.
- Track exceptions on a second tab with end dates.

Growing, with IT or security staff

- Keep 30 to 50 rows, linked to asset IDs and to a ticket per measure.
- Write the authority ladder into the risk policy and have management approve it.
- Quantify two or three close calls a year with three-point estimates.
- Run exceptions through a ticket form that reminds the owner before expiry.

Enterprise or regulated

- Keep a register per entity on group scales and roll them up, as IR 8286C describes[3].
- Score on the ERM scales, so cyber risks join the CRO's register.
- Under DORA's full framework, review the inventory of accepted residual risks at least yearly[11].
- Have internal audit sample acceptances.

Version history

5 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which stated each acceptance rule with its exact scope (2024/2690 for digital providers, Grundschutz++ sign-off by management, DORA's full framework), added the BSI's limits on accepting risks and exceptions and narrowed the FAIR and BSI 200-3 claims.

Sources

1. IR 8286 Rev. 1, Cybersecurity and ERM. NIST, Dec 2025. csrc.nist.gov
2. IR 8286A Rev. 1, Estimating Risk. NIST, Dec 2025. csrc.nist.gov
3. IR 8286C Rev. 1, Staging Risks. NIST, Dec 2025. csrc.nist.gov
4. BSI-Standard 200-3: Risikoanalyse. BSI, Oct 2017. bsi.bund.de
5. BSI-Standard 300-1, v1.0. BSI, 20 Oct 2026. bsi.bund.de
6. NIS-2 Curriculum. BSI, 28 Oct 2026. bsi.bund.de
7. #nis2know: ISO/IEC 27001. BSI, checked 5 Nov 2026. bsi.bund.de
8. NIS2 Directive, Article 21. EUR-Lex, 2022. eur-lex.europa.eu
9. Regulation (EU) 2024/2690. EUR-Lex, 17 Oct 2024. eur-lex.europa.eu
10. NIS2 Implementation Guidance. ENISA, 26 Jun 2025. enisa.europa.eu
11. DORA RTS 2024/1774, Article 3. EUR-Lex, 13 Mar 2024. eur-lex.europa.eu
12. O-RA, Version 2.1. The Open Group, 22 May 2025. publications.opengroup.org