Audit readiness: could you pass an audit without a fire drill?

This quarter, build one evidence register that ties each control to its evidence, owner, location and refresh date, and name one coordinator for every auditor request. Then sample your own controls each quarter and close every finding with a root cause, an owner and a date: ISO certifiers, TISAX, the BSI and DORA all ask for causes and deadlines[2,7,4,9].

Reviewed	Next review	Version	Written for
5 Nov 2026	**5 Dec 2026**	**1.0**	**Security, ISMS and IT leads preparing for ISO 27001, TISAX, BSI, DORA, customer and data protection audits**

Latest version
sheets.einblick.dev/audit-readiness/

If you only do five things

1. **Keep one evidence register.**
   One row per control: requirement, evidence, owner, location, refresh interval and whether a tool collects it. Grundschutz++ asks for each measure's requirement, the date it was done or checked and who checked it[1].
2. **Plan three years of audits at once.**
   ISO 27001 brings surveillance audits in years one and two and recertification in year three[2]. KRITIS proofs[3] and TISAX labels[7] run on 3-year cycles. Book auditors early.
3. **Route every request through one coordinator.**
   Log each request with an ID, the question, the owner, the due time and what was sent. Check every file before it leaves.
4. **Close findings at the root cause, by a date.**
   TISAX requires a root cause and an implementation date for every corrective action and caps each at 9 months[7]. Use the same fields for every audit.
5. **Audit yourself every quarter.**
   Sample key controls as an auditor would: five leavers, three changes, the last restore. IIA cyber audits check that management reviews control failures and fixes them in time[11].

Run an audit without a fire drill

1. **Eight weeks out: what exactly is audited?**
   Confirm scope, criteria, their version and the dates in writing. For a KRITIS proof, agree the scope with the auditor before ordering and put each side's duties in the contract[4].
2. **Six weeks out: is every row current?**
   Refresh stale evidence, rerun the population exports and update open findings. Finish and record the internal audit and management review.
3. **Four weeks out: who answers what?**
   Name a contact per topic[5] and a deputy, and brief them on scope and where the evidence lives. At TISAX level 3, expect unplanned interviews with staff who run the process[7].
4. **Audit days: who sends what?**
   The coordinator sits in on interviews and keeps the request log. Answer only the question asked; if you don't know, say so and follow up.
5. **Each evening and at closing: is it right?**
   Correct misunderstandings with evidence the same day. At the closing meeting, check each finding's facts, grade and clause.

Who can audit you, and what they can demand

- **The BSI, for essential entities.** It can order audits by independent bodies, enter premises during business hours and demand records and answers; wrong answers can cost up to €100,000. From December 2028 it can order proof from any of them[3].
- **The BSI, for KRITIS and important entities.** KRITIS operators submit proof unasked; a wrong, incomplete or late one can cost up to €1 million, ten times that for the company. Important entities face checks only when facts suggest a gap[3].
- **DORA.** Outside microenterprises, internal auditors with ICT expertise and due independence audit the ICT risk framework regularly, management approves the ICT audit plans, and critical findings need a formal follow-up with rules for timely fixes[8].
- **Data protection authorities.** They can order information, run audits and enter premises[12]; in Germany you may refuse self-incriminating answers[13]. Bavaria's BayLDA audits on site, in writing or online and publishes its questionnaires, such as on ransomware[14].
- **Internal audit.** IIA standards require prioritized findings, root causes where possible and tracked follow-up[10]. It can be your KRITIS auditor only with a quality assessment under IDW PS 983 or DIIR No. 3 at most 5 years old[5].
- **Customers.** Serve them from the same register; see the customer assurance sheet.

Audit cycles and deadlines

ISO/IEC 27001 certification

At least one audit each calendar year, surveillance or recertification[2].

Stage 1	Stage 2	Year 1	Year 2	Year 3
Documents and readiness	On site: does it work?	Surveillance audit	Surveillance audit	Recertification

KRITIS proof, BSIG § 39

Counted from the due date, not the submission date[4]; at least two independent auditors[5].

Before due	Due date	Usually quarterly	3 years
Audit and deficiency list	Proof and plan to the BSI	Updated deficiency list	Next proof

Evidence that holds up

- **Populations, not examples.** Export the full list for the period with its query and let the auditor pick. IIA work programs should record population, sample size and method[10]; KRITIS reports explain the sample[5].
- **Exports and live views, not screenshots.** The IIA counts evidence as more reliable when auditors get it directly or from a well-controlled system[10]. Show the setting live, then hand over the export.
- **The whole period, dated.** Label each item with system, query, time and who pulled it. AWS Config returns a resource's compliance at each change[17].
- **Certificates, within limits.** From 2027 one counts toward a KRITIS proof only if its last audit was at most 12 months before the § 39 audit[5].

Between audits

- **Set a refresh interval per row.** Monthly for access and patch exports, quarterly for reviews, yearly for tests and policies. Flag rows past due.
- **Automate what systems record.** Compliance Manager tests improvement actions from Secure Score and Defender for Cloud signals[15]. Beyond its data protection baseline, templates such as ISO/IEC 27001 cost extra; E5 includes three[16].
- **On AWS, use Config conformance packs.** They check technical settings, not policies or procedures[17].
- **Buy a GRC platform for scale.** Our rule: past about 150 rows or three frameworks, with timestamped evidence export.

What you can skip

- **Pre-assessments.** ENX advises against them for TISAX: you pay for two full assessments, even without findings[7].
- **Printed binders.** A read-only folder and a screen share do better.
- **Scripted answers.** They fail at the second question. Brief people on facts and where the evidence is.
- **Monthly evidence for every control.** Refresh by risk instead.

Findings and corrective action

- **ISO 27001.** Majors must be closed before certification, minors need an accepted plan, and a major not verified 6 months after stage 2 repeats it[2].
- **KRITIS.** Fix serious deficiencies at once, minor ones promptly or later with risk treatment[5]. The BSI wants each cause analyzed and can order fixes under penalty[4].
- **TISAX.** Only minor non-conformities with an approved plan get temporary labels. Actions over 3 months need a reason, over 6 months proof they can't be faster, and none may exceed 9 months[7].
- **DORA TLPT.** Within 8 weeks of the authority confirming the test reports are complete, send remediation plans with measures, dates, root causes and owners[9].
- **Old findings return.** The next KRITIS auditor gets your previous list unchanged, with status; open items carry over[5].

What changed in 2026

- **KRITIS proofs every 3 years instead of 2.** Germany's NIS2 law took effect on 6 December 2025; the BSI sent new due dates on 8 December[6]. The law also lets the BSI audit essential entities[3].
- **Stricter KRITIS audit rules.** GAiN 2.2 of 9 July 2026 limits certificate reuse from 2027[5]; binding rules for certified KRITIS auditors are planned for early 2027[4].
- **A cyber baseline for internal audit.** Since 5 February 2026, IIA cyber audits must cover governance, risk and controls[11].
- **AWS Audit Manager closed to new customers** on 30 April 2026[17].

Mistakes that cost the most

- **Evidence made the week before.** Forty access reviews signed on one day show the control didn't run all year.
- **Screenshots without date or source.** They prove a screen, not a control. Grundschutz++ wants tool, time and result for automated checks[1].
- **Controls nobody runs.** A rule with no owner and no record is a finding waiting to happen.
- **Guessing.** Say when you don't know: a wrong answer in a BSI inspection is itself an offense[3]. And a late auditor doesn't excuse a late KRITIS proof[4].

What this looks like at your size

Small team, no security staff

- Keep the register in a spreadsheet and a dated evidence folder per quarter.
- Let your IT provider pull exports, but keep the coordinator role in-house.

Growing, with IT or security staff

- Link each register row to a ticket and collect Microsoft 365 evidence automatically.
- Have someone outside IT operations run the quarterly sample.

Enterprise or regulated

- Plan ISO, KRITIS, TISAX and DORA audits in one three-year calendar from one register.
- Report open findings, overdue actions and expired evidence to management quarterly.

Version history

5 Nov 2026, version 1.0	Published after a copy edit and a source-by-source fact check, which based the ISO 27001 cycle on European Accreditation's quotes of ISO/IEC 17021-1, corrected the BSI's powers and fines for KRITIS and important entities, narrowed TISAX temporary labels and DORA audit duties and added Compliance Manager licensing.

Sources

1. BSI-Standard 300-1, v1.0. BSI, 20 Oct 2026. bsi.bund.de
2. EA FAQs, ISO/IEC 17021-1. EA, checked 5 Nov 2026. european-accreditation.org
3. BSIG §§ 39, 61, 62, 65. BMJV, checked 5 Nov 2026. gesetze-im-internet.de
4. Orientierungshilfe zu Nachweisen. BSI, 30 Oct 2026. bsi.bund.de
5. GAiN, v2.2. BSI, 9 Jul 2026. bsi.bund.de
6. Fragen und Antworten zu NIS-2. BSI, checked 5 Nov 2026. bsi.bund.de
7. TISAX Participant Handbook 2.8. ENX, 13 Mar 2025. enx.com
8. DORA, Articles 5 and 6. EUR-Lex, 14 Dec 2022. eur-lex.europa.eu
9. DORA TLPT standard 2025/1190. EUR-Lex, 18 Jun 2025. eur-lex.europa.eu
10. Global Internal Audit Standards. IIA, 9 Jan 2024. theiia.org
11. Cybersecurity Topical Requirement. IIA, effective 5 Feb 2026. theiia.org
12. GDPR, Articles 31 and 58. EUR-Lex, 27 Apr 2016. eur-lex.europa.eu
13. BDSG § 40. BMJV, checked 5 Nov 2026. gesetze-im-internet.de
14. Datenschutzprüfungen. BayLDA, checked 5 Nov 2026. lda.bayern.de
15. Compliance Manager setup. Microsoft Learn, updated 25 Jun 2026. learn.microsoft.com
16. Compliance Manager regulations list. Microsoft Learn, updated 25 Jun 2026. learn.microsoft.com
17. Audit Manager availability change. AWS, checked 5 Nov 2026. docs.aws.amazon.com