Customer security reviews: can you answer fast without promising more than you do?

This quarter, build one dated evidence pack and one answer library in a standard format such as the CSA CAIQ, and let nothing go out without security's approval. Answer only what is true today, mark planned controls with a date, and accept the clauses NIS2, DORA and the GDPR require while you negotiate how they work.

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

Written for
Sales, security, legal and IT leads at companies that sell to other businesses, especially to EU customers under NIS2 or DORA

Latest version
sheets.einblick.dev/customer-assurance/

If you only do five things

1. **Build one evidence pack.**
   Keep your certificate and scope, audit report, pentest summary, policies, sub-processor list and incident contact in one dated folder. NIS2's implementing rules let cloud and other digital provider customers take audit reports instead of audit rights[1].
2. **Answer from one library in a standard format.**
   Fill in the CSA CAIQ v4.1 once and map every customer form to it. ENISA names the CAIQ and the Shared Assessments SIG as supplier evidence[2].
3. **Answer only what is true today.**
   Mark each control in place, partial or planned with a date, and fix wrong answers at once. In the US, MORSECORP agreed to pay $4.6 million after reporting a near-top NIST SP 800-171 score that was really -142 and fixing it only after a subpoena[3].
4. **Offer your own security terms first.**
   Send a standard addendum with your incident notice time, audit approach, sub-processor notice and data locations with the first questionnaire.
5. **Let security approve every answer.**
   Sales owns the deadline, security the content and legal the contract terms. Nothing goes out without a named approver and a date.

Answer a security review

1. **Which law drives the request?**
   NIS2, DORA, the CRA and the GDPR each push different clauses; the EU security laws sheet covers the first three. The driver decides what you must accept and what you can negotiate.
2. **Does the pack already answer it?**
   Send the pack and the STAR link to your CAIQ first, ideally within five working days, and answer only what they leave open. The third-party risk sheet shows what buyers check.
3. **Which product, entity and sites?**
   Answer for exactly what the customer buys, and say where an answer differs for other products, regions or subcontractors.
4. **Does any answer need a decision?**
   Send every no, partial or new answer to security, and every promise word, such as all, always or within, to legal. Check promised notice times against your incident response plan.
5. **What did you send, and when?**
   Keep the form, the answers, the date and the approver. Review the library every quarter and after major changes, and tell customers before a change makes an answer untrue.

What goes in the evidence pack

- **Certificate and scope.** An ISO/IEC 27001 certificate or TISAX label, scoped to what you sell; see the ISMS sheet. The BSI says no general certificate proves NIS2 compliance[4].
- **A report that tests operation.** SOC 2 or C5 Type 2 tests whether controls worked over a period, Type 1 only their design[5]. For critical functions, DORA customers may rely only on current reports that test key controls in operation[6].
- **Pentest summary.** Date, scope, tester and fix status; see the penetration testing sheet.
- **Product security.** Support period, update policy and component list, which digital providers' purchasing rules must cover under NIS2[1]; see the supply chain sheet.
- **Sub-processors.** Name, service, country and a change feed. Processors must announce changes and let controllers object[8].
- **Company data.** Legal entity, LEI, parent, security contact, service and data countries. DORA registers need each supplier's LEI or EUID, and an LEI outside the EU[9].

Standard formats and their terms

- **CSA CAIQ v4.1.** 283 questions, released in January 2026; STAR accepts v4.0 until December 2027[10]. Submit the STAR Level 1 version, not the reference copy in the CCM workbook[11].
- **The CAIQ license.** CSA's free files are for internal reference and may not be changed or redistributed; commercial use needs a license[11,12]. Cloud providers share it through STAR; ask CSA before emailing the file or building it into a product.
- **Trust page.** Certificates, a SOC 3, which can be freely distributed[7], sub-processors, the security contact and an NDA request form. ENISA points customers to suppliers that publish security commitments[2].
- **AI-CAIQ.** CSA's AI Controls Matrix v1.1 of June 2026 includes one[19]. Use it if you offer AI features, and list which AI services touch customer data.
- **SIG or the customer's own form.** You can answer a customer's SIG, but a SIG of your own needs a Shared Assessments membership or subscription[13]. Answer from the same library, point to your STAR entry or report and keep a copy of what you sent.

On-site audits and right-to-audit requests

- **Agree the scope in writing.** Dates, auditors, agenda and evidence. You may suggest an auditor, but under the GDPR the controller decides[16].
- **Offer remote first.** The EDPB expects both sides to agree in good faith whether a visit is needed, weighing security; the controller has the final say[16].
- **Charge fairly.** The EDPB says contracts shouldn't set audit fees so high that they deter audits[16].
- **Protect other customers.** Show evidence on screen, escort visitors and keep other customers' data out of reach. Close findings by a date.

What changed in 2026

- **Germany's NIS2 law took effect on 6 December 2025.** About 29,500 companies and federal bodies have new duties[4]. The BSI says they must bind suppliers to security requirements and may have to drop those who can't meet them[17].
- **C5:2026 applies from 1 June 2027.** Until then, reports dated or ending from 28 February 2027 must describe planned changes[5].
- **CRA duties reach suppliers.** Since 11 September 2026, manufacturers must report actively exploited vulnerabilities; from 11 December 2027 they must exercise due diligence on third-party components[18].

Contract clauses: accept, negotiate or push back

Accept: the law requires them

- **Processor audits.** Allow and contribute to audits and inspections by the controller or its auditor[8].
- **Digital provider customers under NIS2.** Security requirements, incident notice without undue delay, vulnerability handling, audits or reports, subcontractor and exit rules, where appropriate[1].
- **DORA terms.** Data locations, incident help at no extra or preset cost, supervisor cooperation and exit support; for critical or important functions, unrestricted audit and access rights and threat-led tests[14].

Negotiate the details

- **Incident notice.** Agree a trigger, such as a confirmed incident, and a time, such as 24 hours.
- **Audit form.** Reports first, then remote[16] or pooled audits[6]; DORA allows alternative assurance if other clients' rights are affected[14].
- **Sub-processor changes.** Notice and a right to object, not approval of each one. For DORA critical functions, an ignored objection allows termination[15].
- **Data location.** Commit to countries for storage and processing; DORA registers record both[9].

Push back

- **Unlimited liability.** Ask legal to cap it and match it to your cover; see the cyber insurance sheet.
- **Your policy, as amended.** Accept a dated annex; you can't comply with changes you haven't seen.
- **Tests of your shared systems.** Offer your pentest summary and let the customer test its own tenant under your rules.
- **Audits on demand.** Outside DORA, offer one a year with 30 days' notice, plus one after a serious incident or at a regulator's request.

What you can skip

- **A new answer set for each customer.** Map each form to one library.
- **Certificates nobody asks for.** Get the one key customers name.
- **Waiting for an EU cyber posture certificate.** The Commission proposed one in January 2026[20]; Parliament is still at committee stage[21].
- **Questionnaire software before the library.** A dated folder and a spreadsheet of approved answers carry you through the first year.

Mistakes that cost the most

- **Saying yes to close the deal.** The US FTC barred GoDaddy from misrepresenting its security after alleging it claimed award-winning security without MFA[22]. In Germany, a customer deliberately deceived into signing can void the contract[23].
- **The wrong scope.** An office certificate doesn't cover a hosted service.
- **Notice times nobody can meet.** A two-hour clock without on-call staff breaks the contract on the first weekend.
- **Answers from a tool or template.** They describe controls you don't run.

What this looks like at your size

Small team, no security staff

- Fill in the CAIQ v4.1 once and keep it with a dated evidence folder.
- Use a CyberRisikoCheck under DIN SPEC 27076 as a start, not as NIS2 proof[17].

Growing, with IT or security staff

- Publish a trust page with an NDA request form and a sub-processor feed.
- Agree a standard security addendum and fallback positions with legal.

Enterprise or regulated

- Keep a DORA data sheet with your LEI, parent, countries and subcontractors[9].
- Track requests in one queue with an answer library, owners and expiry dates.

Version history

5 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which limited NIS2 supplier clauses to customers that are digital providers, applied CSA's and Shared Assessments' license terms to sharing questionnaires and scoped the DORA clauses to critical functions.

Sources

1. Regulation (EU) 2024/2690. EUR-Lex, Oct 2024. eur-lex.europa.eu
2. Technical Implementation Guidance (NIS2). ENISA, Jun 2025. enisa.europa.eu
3. MORSECORP to pay $4.6 million (US). US DOJ, 26 Mar 2025. justice.gov
4. Fragen und Antworten zu NIS-2. BSI, checked 5 Nov 2026. bsi.bund.de
5. Kriterienkatalog C5: FAQ. BSI, checked 5 Nov 2026. bsi.bund.de
6. DORA RTS (EU) 2024/1773, Art. 8. EUR-Lex, 13 Mar 2024. eur-lex.europa.eu
7. SOC 3 reports. AICPA & CIMA, checked 5 Nov 2026. aicpa-cima.com
8. GDPR, Article 28. EUR-Lex, 27 Apr 2016. eur-lex.europa.eu
9. DORA ITS 2024/2956, Annex I. EUR-Lex, Nov 2024. eur-lex.europa.eu
10. CCM v4.1 transition timeline. CSA, 19 Feb 2026. cloudsecurityalliance.org
11. Cloud Controls Matrix v4.1. CSA, 27 Jan 2026. cloudsecurityalliance.org
12. CCM & AICM Licensing FAQ. CSA, 13 Mar 2026. cloudsecurityalliance.org
13. SIG FAQ. Shared Assessments, Aug 2025. sharedassessments.org
14. DORA, Article 30. EUR-Lex, 14 Dec 2022. eur-lex.europa.eu
15. DORA RTS (EU) 2025/532, Art. 6. EUR-Lex, 24 Mar 2025. eur-lex.europa.eu
16. Guidelines 07/2020: controller, processor. EDPB, Sep 2022. edpb.europa.eu
17. #nis2know: Sichere Lieferkette. BSI, checked 5 Nov 2026. bsi.bund.de
18. Cyber Resilience Act, Art. 13, 14, 71. EUR-Lex, Oct 2024. eur-lex.europa.eu
19. AI Controls Matrix v1.1. CSA, 22 Jun 2026. cloudsecurityalliance.org
20. Cybersecurity Package: Q&A. EU Commission, 20 Jan 2026. digital-strategy.ec.europa.eu
21. 2026/0011(COD): Cybersecurity Act 2. European Parliament, checked 5 Nov 2026. oeil.europarl.europa.eu
22. FTC finalizes order with GoDaddy (US). FTC, 21 May 2025. ftc.gov
23. BGB § 123. BMJV (Germany), checked 5 Nov 2026. gesetze-im-internet.de