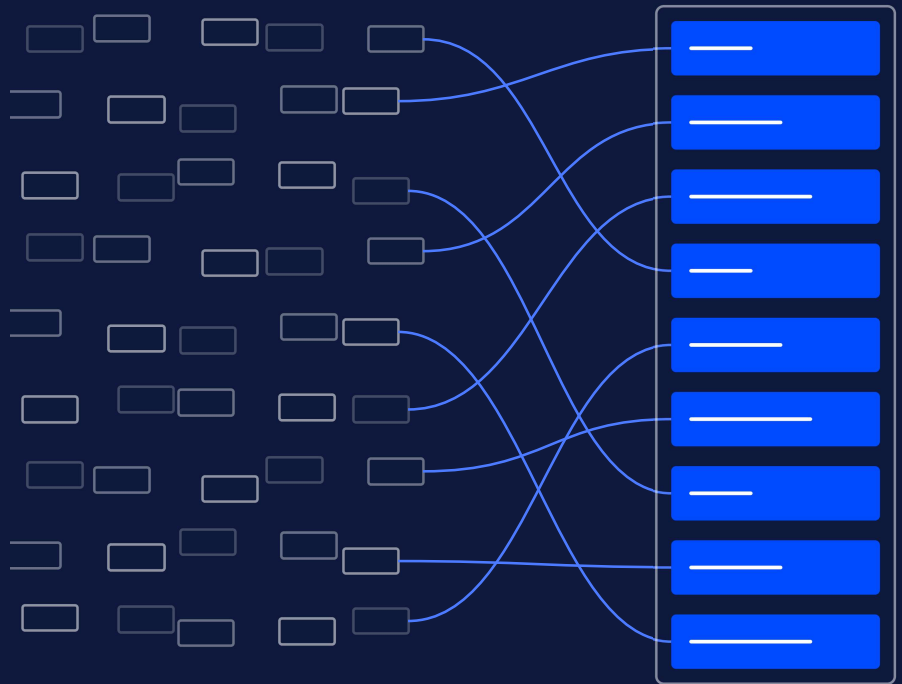




SECURITY AND GRC TOOLKIT

The Security Questionnaire Response Kit

Turn every customer security questionnaire into a retrieval job.

Seven tools for security, GRC and compliance teams: a readiness scorecard, evidence library checklist, control matrix, six-stage workflow, answer patterns, pre-submission QA and a review calendar.

Matt Davies, Chief Product Officer, SureCloud

Technically reviewed by **Gabriel Few-Wiegratz**, [job title], SureCloud

Version 1.0 · August 2026

How to use this kit

Who it's for

Security, GRC and compliance leads who answer customer security questionnaires. And the sales, bid and account teams who wait on them.

How it works

Start with the scorecard. It takes ten minutes and tells you which tools to open first.

Every tool is built to be printed, copied into your own templates, or rebuilt inside your GRC platform. The control matrix is also available as a spreadsheet: [link to companion template].

What you'll have at the end

- **One evidence library.** Current, dated, owned.
- **One control matrix.** Every question mapped to a control, a piece of evidence and a named owner.
- **One repeatable process.** Six stages, clear owners, no night-before drafting.

CONTENTS

	Why questionnaires still take weeks	3
Tool 01	Readiness scorecard	4
Tool 02	Evidence library checklist	5
Tool 03	Control matrix	7
Tool 04	Six-stage response workflow	9
Tool 05	Answer patterns	10
Tool 06	Pre-submission QA checklist	12
Tool 07	Review cadence calendar	13
	Reduce the volume, and where to start	14
	Where SureCloud fits	15

Fast answers come from maintained evidence.
Not faster writing.

The questionnaire isn't the hard part. Finding the evidence is.

Teams that answer in hours are retrieving answers they already maintain. Teams that take weeks are drafting from scratch under deadline. That's where the errors creep in: expired certificates, contradictory timelines, sub-processor lists nobody has checked since the last renewal.

! 01

Consistency drift

Several people contribute. Their answers disagree. One section says incidents are notified within 24 hours, another says 72. Nobody reads a 200-question response end to end, so the contradiction ships.

! 02

Evidence fragmentation

Policies in SharePoint. Certificates in someone's inbox. Audit reports on a file server. Every questionnaire restarts the hunt, and the hunt takes most of the time.

! 03

Stale answers under pressure

Short deadlines push teams to copy last year's response. Certificates expire. Policies change. Sub-processors change. The copied answer is now wrong.

Why now: your answers now outlive the deal

Buyers aren't asking more often because they're curious. Regulation is making supplier due diligence a formal, recurring obligation.

DORA, Article 28.

Since 17 January 2025, EU financial entities must assess ICT third-party providers before contracting (Article 28(4)) and keep a register of information on those arrangements, report on it to regulators at least yearly and share it in full on request (Article 28(3)).

NIS2, Article 21(2)(d).

Essential and important entities must manage supply chain security, including the security of their relationships with direct suppliers and service providers.

UK GDPR, Article 28(1).

Controllers may only use processors that provide sufficient guarantees of appropriate technical and organisational measures.

The result: questionnaires are written into contracts, revisited at renewal, and treated as a compliance activity rather than a sales one.

EXPERT VIEW

"Buyers can tell the difference between an answer pulled from a maintained control set and one written the night before. The tell is usually the sub-processor list: it changes more often than anything else and gets updated least."

MATT DAVIES, CHIEF PRODUCT OFFICER, SURECLOUD

Readiness scorecard

Find out how far you are from answering questionnaires in hours, not weeks.

Use it when: before your next questionnaire lands

Time needed: 10 minutes

Owner: GRC or security lead

Score each statement honestly. 0 = no. 1 = partly, or true but not evidenced. 2 = yes, and we could prove it today.

#	Statement	0	1	2	Fix with
1	Our current certifications and audit reports sit in one place, with expiry dates and a named owner.	☐	☐	☐	Tool 02
2	Every security policy is dated, version-controlled and has a next review date.	☐	☐	☐	Tool 02
3	We can produce our latest access review, vulnerability scan and penetration test summary within an hour.	☐	☐	☐	Tool 02
4	Our sub-processor list is current, shows data residency, and was reviewed in the last quarter.	☐	☐	☐	Tool 02
5	We have a dated data processing agreement template with transfer mechanisms noted.	☐	☐	☐	Tool 02
6	Incident contacts, notification timeframes and escalation routes are documented with named people and stated hours.	☐	☐	☐	Tool 02
7	We have a control matrix that maps incoming questions to controls, evidence and owners.	☐	☐	☐	Tool 03
8	That matrix is mapped to ISO/IEC 27001:2022 Annex A or the SOC 2 Trust Services Criteria.	☐	☐	☐	Tool 03
9	Every questionnaire section has a named owner by domain.	☐	☐	☐	Tool 04
10	A named person signs off every response before it leaves the business.	☐	☐	☐	Tool 04
11	Every stored answer has an owner and a review date.	☐	☐	☐	Tool 07
12	We publish a standard answer set, such as a CAIQ on the CSA STAR Registry or a Trust Centre, that buyers can check first.	☐	☐	☐	Page 14

Your score: _____ / 24

! 0 to 8

Drafting from scratch

Every questionnaire restarts the hunt. Start with Tool 02 and Tool 03. Build the library before you build the process.

9 to 16

Partly retrievable

The evidence exists but the process doesn't. Start with Tool 04 and Tool 06. Owners and a QA step will remove most of your rework.

✓ 17 to 24

A retrieval job

Keep it that way. Start with Tool 07, then look at reducing how many questionnaires you receive (page 14).

Evidence library checklist

Everything a buyer is likely to ask for, gathered once, dated and owned.

Use it when: building or auditing your library

Time needed: half a day to audit

Owner: GRC lead, with domain owners

An expired certificate cited in a response damages credibility faster than a missing one. For every item, record where it lives, who owns it and when it is next reviewed.

A. Certifications and audit reports

Evidence item	What “current” looks like	Suggested cadence	Owner	Next review
☐ ISO/IEC 27001 certificate	Scope and expiry date recorded. Scope covers the services you sell.	Each audit cycle	_____	_____
☐ Statement of Applicability	Matches the current certificate and version.	Each audit cycle	_____	_____
☐ SOC 2 Type 2 report	Report period recorded. Bridge letter ready for the gap since the period ended.	Each report cycle	_____	_____
☐ PCI DSS Attestation of Compliance (if card data is in scope)	In date and matches the scope you describe.	Annual	_____	_____

B. Security policies Each one dated, version-controlled, approved and owned.

Evidence item	What “current” looks like	Suggested cadence	Owner	Next review
☐ Information security policy	Approved by leadership, version and date on the document.	Annual	_____	_____
☐ Access management policy	Covers joiners, movers, leavers, MFA and privileged access.	Annual	_____	_____
☐ Data classification policy	Classification levels match how you describe data in answers.	Annual	_____	_____
☐ Acceptable use policy	Covers personal devices, remote working and AI tools.	Annual	_____	_____
☐ Incident response policy and plan	Notification timeframes stated in hours.	Annual	_____	_____
☐ Business continuity plan	States recovery time and recovery point objectives.	Annual	_____	_____

D. Third-party documentation

Evidence item	What “current” looks like	Suggested cadence	Owner	Next review
☐ Sub-processor list	Every sub-processor, what they process, and data residency.	Quarterly	_____	_____
☐ Vendor risk assessment process	Documented process plus recent completed assessments.	Annual	_____	_____

C. Control evidence

	Evidence item	What “current” looks like	Suggested cadence	Owner	Next review
☐	Access review logs	Latest review signed off, with actions closed.	Quarterly	_____	_____
☐	Vulnerability scan results	Latest cycle, dated, with remediation status.	Per scan cycle	_____	_____
☐	Penetration test summary	Shareable executive summary, dated, with remediation status.	Annual, and after major change	_____	_____
☐	Encryption configuration records	At rest and in transit, matching the standards you quote.	Annual, and on change	_____	_____
☐	Patch management reports	Latest period, with exceptions explained.	Monthly	_____	_____
☐	Disaster recovery test results	Last test date, outcome and actions.	Annual	_____	_____

E. Data protection

	Evidence item	What “current” looks like	Suggested cadence	Owner	Next review
☐	Data processing agreement template	Dated, with transfer mechanisms noted (for example the UK IDTA or UK Addendum, EU SCCs).	Annual, and on regulatory change	_____	_____
☐	Data retention schedule	Retention periods match what you state in answers.	Annual	_____	_____

F. Incident response

	Evidence item	What “current” looks like	Suggested cadence	Owner	Next review
☐	Incident contacts and escalation	Named people, deputies, notification timeframes in hours, escalation route.	Quarterly	_____	_____

G. AI systems

	Evidence item	What “current” looks like	Suggested cadence	Owner	Next review
☐	AI system inventory	Which AI systems and model providers touch customer data, for what purpose, and where.	Quarterly	_____	_____

2 Two items go stale fastest. The sub-processor list and the AI system inventory change more often than anything else in the library. Put them on a quarterly cycle and review them whenever you onboard a new vendor or ship a new AI feature.

Control matrix

Answer the same control once, whatever format the buyer sends.

Use it when: after the evidence library is in place

Time needed: first version over several working sessions

Owner: GRC lead

Why it matters

The control matrix is generally the single most valuable thing to build before the next questionnaire arrives. It cross-references each incoming question to the control that answers it, the evidence behind that control, and the person who owns it.

Map your controls to ISO/IEC 27001:2022 Annex A or the SOC 2 Trust Services Criteria and they become reusable across buyer formats. It also stops your own answers contradicting each other.

How to build the first version

- 1 Collect.** Export the last three questionnaires you answered.
- 2 Group.** Put repeated questions under one control statement, written in your own words.
- 3 Map.** Link each control statement to ISO/IEC 27001:2022 Annex A, the SOC 2 Trust Services Criteria, or both.
- 4 Evidence.** Attach one current piece of evidence and name one owner.
- 5 Approve.** Write the standard answer once, have it approved, and give it a review date.



Column guide

ID: your reference, for example AC-01.

Domain: access controls, data protection, incident response, business continuity, third-party risk, compliance and certification.

Control statement: what you do, in plain language.

ISO/IEC 27001:2022: Annex A control references.

SOC 2: Trust Services Criteria references.

Evidence: file name, location and date.

Owner: a named role, not a team.

Review: last reviewed and next review date.

Approved answer: the wording you reuse.

Worked examples

ID	Domain	Control statement	ISO/IEC 27001:2022	SOC 2	Evidence	Owner	Review
AC-01	Access controls	MFA is enforced for all workforce access to production systems and corporate SaaS.	A.5.17, A.8.5	CC6.1	Identity provider policy export, dated	IT security lead	Quarterly
DP-01	Data protection	Customer data is encrypted at rest and in transit to [standards].	A.8.24	CC6.1, CC6.7	Encryption configuration record, dated	Head of infrastructure	Annual
IR-01	Incident response	Customers are notified of a confirmed incident affecting their data within [X] hours.	A.5.24, A.5.26	CC7.3, CC7.4	Incident response plan v[X], contact list	Head of security	Quarterly
BC-01	Business continuity	[Service] has an RTO of [X] hours and RPO of [X] hours, tested annually.	A.5.29, A.5.30, A.8.13	A1.2, A1.3	DR test report, dated	Business continuity owner	Annual
TP-01	Third-party risk	Sub-processors are risk-assessed before onboarding; the list is reviewed quarterly.	A.5.19, A.5.21, A.5.22	CC9.2	Sub-processor list, assessment records	Vendor risk manager	Quarterly
CC-01	Compliance and certification	Certified to ISO/IEC 27001:2022 for [scope], valid until [date].	A.5.35	CC4.1	Certificate, Statement of Applicability	GRC lead	Each audit cycle

References are illustrative starting points. Confirm mappings against your own Statement of Applicability and SOC 2 system description.

Six-stage response workflow

The same six steps for every questionnaire, with a named owner at each one.

Use it when: every time a questionnaire arrives

Time needed: set up once

Owner: questionnaire coordinator

01 Intake

What happens

Log the sender, format, deadline and estimated effort. Mark each section as retrieve or write. Set an internal deadline 48 hours before the buyer's.

Owner

Questionnaire coordinator

Output

Intake log entry

Done when

Every section is marked retrieve or write.

02 Triage

What happens

Assign each section to its function. Flag questions nobody can answer now, not on deadline day.

Owner

Questionnaire coordinator

Output

Owner map

Done when

Every section has a named owner and a date.

03 Draft

What happens

Pull from the control matrix first. Reference policies and attach audit reports. Write new answers only where no approved answer exists.

Owner

Domain owners

Output

First draft with evidence references

Done when

No blank answers, no unevidenced claims.

04 Review

What happens

Security and compliance leads check consistency and alignment with certifications. Legal reviews contractual implications. Catch contradictions between answers and audit reports.

Owner

Security lead, compliance lead, legal

Output

Reviewed draft

Done when

Tool 06 checklist passes.

05 Approve and deliver

What happens

A named owner signs off. Sensitive evidence is redacted. The version is recorded internally.

Owner

Named approver

Output

Submitted response

Done when

Sign-off and version are recorded.

06 Archive and update

What happens

Store the final response. Any answer written fresh goes into the control matrix with an owner and review date.

Owner

Questionnaire coordinator

Output

Updated matrix

Done when

Next time, that answer is a retrieval.

Intake log fields

Buyer	
Buyer contact	
Format (SIG, CAIQ, portal, spreadsheet, other)	
Number of questions	
Date received	
Buyer deadline	
Internal deadline	
Deal stage	
Coordinator	
Status	

Section ownership by domain

Domain	Typical owner
Access controls	Security team
Data protection and privacy	DPO
Incident response	Head of security
Business continuity	Business continuity owner
Third-party risk	Vendor risk manager or DPO
Compliance and certification	GRC or compliance lead
Contractual terms	Legal

Answer patterns

Specific beats reassuring. Patterns for the questions every buyer asks.

Use it when: drafting or refreshing standard answers

Time needed: 5 minutes per answer

Owner: domain owners

Anatomy of a trusted answer

1 What you do

1. Do you enforce multi-factor authentication?

Yes. MFA is enforced for [all workforce accounts] accessing [production systems and corporate SaaS] through [identity provider]. Enforcement is reviewed [quarterly] by [role].

Attach: identity provider policy export, dated.

2 Where it applies

3 How often

4 What proves it

2. Is customer data encrypted at rest and in transit?

Yes. Customer data is encrypted at rest using [standard] and in transit using [protocol and minimum version]. Keys are managed in [service] and rotated [frequency].

Attach: encryption configuration record, dated.

3. How quickly will you notify us of a security incident?

We notify affected customers of a confirmed incident within [X] hours, through [channel], via [named role]. This matches the timeframe in our data processing agreement.

Attach: incident response plan, version and date.

4. Do you hold a current certification or audit report?

Yes. We are certified to ISO/IEC 27001:2022 for [scope], valid until [date]. Our SOC 2 Type 2 report covers [period]; a bridge letter covers [period].

Attach: certificate, Statement of Applicability, report under NDA.

5. Do you carry out independent penetration testing?

Yes. [Provider type] tests [scope] [frequency]. The last test completed in [month and year]. All high and critical findings were remediated by [date].

Attach: executive summary.

6. How do you manage sub-processors?

Every sub-processor is assessed before onboarding and reviewed [annually]. Our list, including data residency, is reviewed quarterly and published at [location]. We notify customers of changes [X] days in advance.

Attach: sub-processor list, dated.

7. What are your recovery time and recovery point objectives?

For [service], our RTO is [X] hours and our RPO is [X] hours. We last tested recovery on [date]; the test [met / did not meet] objectives, with actions [status].

Attach: DR test summary.

8. Do you use AI with our data?

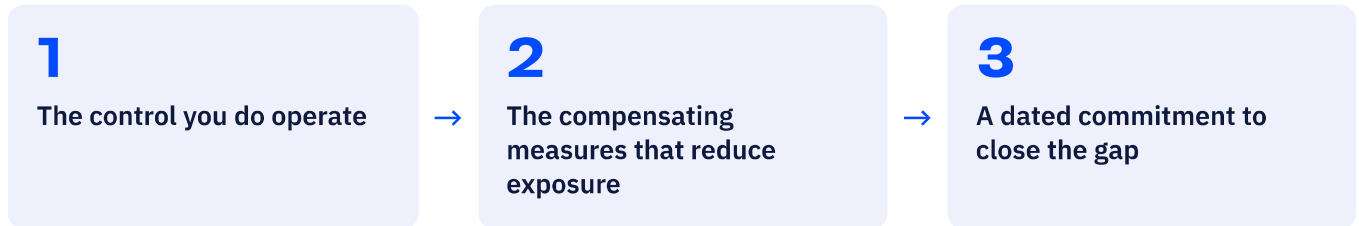
[Describe the AI systems and model providers that process customer data, and for what purpose.] Customer data [is / is not] used to train models. Use of AI is governed by [policy] and recorded in our AI system inventory, reviewed quarterly.

Attach: AI use policy, inventory extract.

When the honest answer is “not yet”

Overstated answers are how questionnaires turn into full buyer-led assessments. A gap handled well builds more trust than a claim that falls apart under testing.

The three-part gap answer



Worked examples

Access reviews are manual

“Quarterly access reviews are manual today, with privileged access logged and reviewed weekly, and automation scheduled for Q2.”

No SOC 2 report yet

“We don’t hold a SOC 2 report today. Our controls are certified to ISO/IEC 27001:2022 for [scope], valid until [date], and we can share our Statement of Applicability under NDA. A SOC 2 readiness assessment is scheduled for [quarter].”

Penetration test is overdue

“Our last independent penetration test completed in [month and year]. Since then, [authenticated vulnerability scanning] has run [monthly], with high and critical findings remediated within [X] days. Our next test is booked for [month and year].”

No formal AI system inventory

“We are formalising our AI system inventory. Today, use of AI with customer data is restricted by [policy] and approved case by case by [role]. The inventory will be complete by [date].”

! Words that trigger a deeper assessment

- “always”
- “all”
- “never”
- “fully compliant”
- “100%”
- “bank-grade”
- “military-grade”

Use them only when you can evidence them.

Pre-submission QA checklist

! **The contradiction hunt.** Run it before anything leaves the business.

Use it when: stage 04, Review

Time needed: 30 to 60 minutes

Owner: security or compliance lead

#	Check	Initials
☐ 01	Every certificate cited is in date, and its scope covers the service this buyer is buying.	_____
☐ 02	The SOC 2 report period is stated, with a bridge letter for the gap since it ended.	_____
☐ 03	The incident notification timeframe is identical everywhere it appears: questionnaire, DPA, contract, Trust Centre.	_____
☐ 04	RTO and RPO match the business continuity plan and the last DR test.	_____
☐ 05	The sub-processor list matches the DPA and your published list, including data residency.	_____
☐ 06	Encryption standards quoted match the configuration records.	_____
☐ 07	No answer claims a control that your audit report lists as an exception.	_____
☐ 08	Policy names and version numbers match the documents attached.	_____
☐ 09	Every “No” or “Partial” uses the three-part gap answer.	_____
☐ 10	No absolutes (“always”, “all”, “never”, “100%”) without evidence.	_____
☐ 11	Sensitive evidence is redacted: internal hostnames and IP addresses, personal data, detailed test findings.	_____
☐ 12	A named approver has signed off and the version is recorded internally.	_____

SIGN-OFF

Questionnaire:

Buyer:

Approved by:

Date:

Version:

Review cadence calendar

Every answer gets an owner and a review date. Then it stays true.

Use it when: after the matrix is built

Time needed: 1 hour to set up

Owner: GRC lead

Review at least annually, and immediately when a control, certification or sub-processor changes. Set each review as a compliance task with a named owner, not a calendar reminder someone can ignore.

Answer category	Suggested cadence	Also review when	Owner
Sub-processor list	Quarterly	A vendor is onboarded or changes hosting region	_____
AI system inventory	Quarterly	A new AI feature or model provider goes live	_____
Incident contacts	Quarterly	Anyone in a named role changes	_____
Published answers (CAIQ, Trust Centre)	Quarterly	Any item in this table changes	_____
Certifications and audit reports	Each audit cycle; flag 90 days before expiry	Scope changes	_____
Security policies	Annual	Major organisational or regulatory change	_____
Encryption configuration	Annual	Architecture change	_____
RTO and RPO	Annual, after the DR test	A major incident or infrastructure change	_____
Penetration test summary	Annual	A major release or architecture change	_____
DPA and transfer mechanisms	Annual	Regulatory change affecting transfers	_____

Q1	Q2	Q3	Q4
- Quarterly items ○ _____ ○ _____ ○ _____	- Quarterly items ○ _____ ○ _____ ○ _____	- Quarterly items ○ _____ ○ _____ ○ _____	- Quarterly items ○ _____ ○ _____ ○ _____

Answer fewer questionnaires

The fastest questionnaire is the one a buyer doesn't send. Give them a trusted, current answer set to check first.

1

Publish a CAIQ to the CSA STAR Registry

If you offer cloud services, a STAR Level 1 self-assessment using the Consensus Assessments Initiative Questionnaire (CAIQ) answers a large share of what buyers ask. Sales can point buyers to it and keep follow-ups short.

2

Run a Trust Centre

Publish current certifications, policy summaries and your sub-processor list in one place. Keep detailed reports behind an NDA request.

3

Send the standard pack first

Before a bespoke questionnaire arrives, offer your certificate, Statement of Applicability, CAIQ, penetration test summary and sub-processor list.

Keep it current. A published answer that is out of date does more damage than no published answer at all.

Where to start: a 90-day plan



Days 1 to 30

- ☐ Run the readiness scorecard (Tool 01)
- ☐ Centralise certifications and audit reports with expiry dates and named owners (Tool 02)



Days 31 to 60

- ☐ Build the control matrix, mapped to ISO/IEC 27001:2022 Annex A or SOC 2 (Tool 03)
- ☐ Define the six-stage workflow and assign section owners by domain (Tool 04)



Days 61 to 90

- ☐ Set review cadences for every answer category as compliance tasks (Tool 07)
- ☐ Publish your CAIQ to the STAR Registry or launch a Trust Centre

A spreadsheet matrix goes stale. A maintained control framework doesn't.

This kit works in a spreadsheet. At volume, spreadsheets drift, owners change and evidence goes out of date between questionnaires. That's the point where teams move the matrix into a platform.



Map once. Reuse everywhere.

SureCloud Compliance Management maintains your control framework continuously. Map a control once across ISO/IEC 27001, SOC 2, DORA and more, and reuse the evidence in every response.



The mapping gets done for you.

Gracie AI Agents with Personas and Skills perform the mapping and assessment activities, with every action logged. AI operates the role. Humans lead the programme.



Buyers check before they ask.

SureCloud Trust Centre publishes your current certifications and documents in one place, so fewer buyers need to send a questionnaire at all.

50–65%

reduction in manual evidence collection effort with SureCloud Compliance Management.

Book a demo · [\[demo URL\]](#)



[QR code placeholder]

Scan to see SureCloud Compliance Management

ABOUT THE AUTHORS

Matt Davies, Chief Product Officer, SureCloud

[40-word bio: years in GRC and product leadership, areas of focus, relevant credentials.]

Gabriel Few-Wiegratz, [job title], SureCloud

[40-word bio: GRC practice experience, frameworks worked with, certifications such as ISO 27001 Lead Auditor if held.]

About SureCloud

SureCloud is the GRC platform that does more, better, with less. Founded in London in 2006, SureCloud brings risk, compliance, audit, third-party risk, business continuity and privacy into one platform.

Sources

Regulation (EU) 2022/2554 (DORA), Article 28 · Directive (EU) 2022/2555 (NIS2), Article 21(2)(d) · UK GDPR, Article 28(1) · ISO/IEC 27001:2022, Annex A · AICPA Trust Services Criteria · Cloud Security Alliance, STAR Registry and CAIQ v4

Disclaimer

This kit is practical guidance, not legal advice. Framework references reflect ISO/IEC 27001:2022 and the AICPA Trust Services Criteria at the time of publication.

Next questionnaire in the inbox? **Make it a retrieval job.**

See how SureCloud keeps your control framework, evidence and answers current, so your team spends its time on the questions that need judgement.

Book a demo · [demo URL]



Read the full guide: How to prepare for a customer security questionnaire

surecloud.com/blog-hub/customer-security-questionnaire

Your Business Assured.

