

Clear answers. Supporting evidence.

Sample security assurance deliverables

A worked example of a customer questionnaire response pack, a supplier review and a focused readiness review.

Inside this pack

1. Customer questionnaire responses, evidence register and handover
2. Supplier due diligence findings and decision record
3. Focused readiness findings and action plan

Fictional examples. These are not client findings, verified controls or approved responses.

Every organisation, document and control described in these examples is invented. A real engagement has an agreed scope and evidence basis. The client approves responses and owns supplier and risk decisions.

Fidelis Iwu trading as Firmword
hello@firmword.co.uk

Firmword sample deliverables

Fictional examples. These are not client findings, verified controls or approved responses.

Fictional questionnaire example

Client: Example SaaS Ltd. Product: ExampleDesk. Buyer: Example Buyer Ltd. Version: demonstration 1.

Status: awaiting client approval. Every document and fact below is invented.

Question	Draft response	Evidence and status
Q01 Is MFA enforced for all access?	MFA is enforced for workforce administrative access. Customer-account MFA is optional. Do not answer an unqualified Yes.	EV01 access policy section 3 and EV02 configuration excerpt. Partially supported. CTO must confirm coverage.
Q02 Is production storage encrypted?	The documented production database and object store use encryption at rest. Exports and endpoints are outside this evidence scope.	EV03 architecture section 4 and EV04 storage excerpt. Supported for stated scope, awaiting approval.
Q03 Has recovery been tested recently?	A backup procedure has been supplied. No dated restore-test result has been provided, so recent successful recovery cannot yet be confirmed.	EV05 backup procedure. Not evidenced. Engineering owner to supply test record or confirm gap.

Evidence register and actions

EV01: Access control policy v1.2, 15 September 2026. EV02: Admin MFA configuration excerpt, 29 September 2026. EV03: Architecture v2.0, 10 September 2026. EV04: Storage configuration excerpt, 29 September 2026. EV05: Backup procedure v1.0, 1 August 2026. Evidence locations and owners must be recorded in a real engagement.

GAP01: CTO confirms the exact MFA coverage before approving Q01. GAP02: Engineering provides restore evidence before Q03 can claim a successful test. Do not add remediation dates without agreement.

Answer library and handover

ANS01 is the scoped encryption answer from Q02. Record exact wording, product, EV03 and EV04, approver, approval date and review trigger. Its status remains Draft until approved. Review when storage or hosting changes. Deliver the original-format form, register and open actions together. The client approves and submits to the buyer.

Fictional supplier due diligence example

Client: Example SaaS Ltd. Supplier: Example Support Cloud Ltd. Intended use: customer support tickets. Data: business contact details and ticket content, which may contain customer personal data. Access: scoped application integration. Business dependency: medium. These facts and documents are invented.

Finding	Basis and consequence	Required next step
Certificate scope needs confirmation	SV01 is a certificate excerpt for a different legal entity. It does not yet establish coverage of the proposed service.	Ask for certificate, scope schedule and link between the contracting entity and certified service.
Subprocessor information incomplete	SV02 processing terms mention subprocessors but do not include a current list or transfer locations.	Obtain the current list and relevant transfer terms. Client legal/privacy owner reviews suitability.
Recovery performance not evidenced	SV03 continuity policy describes backups but gives no recent test result for the proposed service.	Request a service-specific recovery summary and measured test results.
Integration access can be reduced	SV04 proposed permissions include write access beyond the intended ticket synchronisation.	Client engineering owner tests the minimum permissions and confirms the required access.

Recommendation and decision record

Recommendation: complete the evidence and permissions checks before production use. An excerpt alone is insufficient to confirm certificate coverage. Do not label the supplier insecure solely because a document is missing. The client decides whether conditions, alternatives or acceptance of residual risk are appropriate.

Decision fields: supplier/service version, reviewer, documents and dates, recommendation, client decision owner, accepted conditions, residual risks, decision date and next review trigger. Decision: pending. Risk acceptance: pending. Re-review if data use, access, subprocessors or service scope changes.

Fictional focused readiness example

Client: Example SaaS Ltd. Product: ExampleDesk. Review scope: five agreed customer security requirements. This is a selected-requirement review, not a comprehensive ISO 27001 assessment. Policies and claims below are invented.

Requirement	Finding	Action and evidence for closure
Access removal	RR01 policy sets an offboarding process. No completed removal record supplied. Partially supported.	Operations records a real completed leaver check. Client confirms scope and removes unnecessary personal data.
MFA for privileged access	RR02 configuration shows the main admin group. Service accounts not covered by the excerpt. Not evidenced for complete coverage.	Engineering documents the privileged account inventory and appropriate authentication controls.
Recovery testing	RR03 backup procedure exists. Client confirms no recent restore test. Confirmed gap.	Engineering agrees and performs a safe restore exercise, retains dated results and records actions.
Incident handling	RR04 incident procedure names an owner. Exercise or incident evidence not supplied. Partially supported.	Operations validates current contacts and retains exercise notes with follow-up actions.
Supplier reviews	RR05 shows a supplier list. No review record for the support supplier. Not evidenced.	Procurement completes a scoped review before production use and records the client decision.

Priority and planning

Address access coverage and supplier checks before granting relevant production access. Agree recovery testing with engineering based on business impact and safe test conditions. Validate incident contacts next. These priorities follow the fictional use case, not a regulatory risk rating. Set owners and dates with the client. Missing evidence remains open until adequate closure evidence is reviewed.

Record each action with ID, requirement, evidence basis, owner, target date, status, closure evidence and reviewer. Use Open, In progress, Awaiting evidence or Closed. Never change an item to Closed just because a task was assigned.