



Security Partner Delivery Pack

Illustrative Scope Review and Client Handoff

DevBrows | Public sample v1.0 | 9 October 2026

Use this pack to agree how a first referral or co-delivery project would run. It contains a worked SaaS and AI scope, a report outline, release checks, and a handoff plan. The engagement names the people responsible and confirms capacity before dates are committed.

Illustrative planning material. ExampleSaaS Sandbox, its identities, findings and retest outcomes are fictional. No client engagement or executed assessment is represented. The sample is not a signed proposal, completed review or commitment to a delivery date.

Read the pack alongside the demonstration report

The separate 17-page demonstration report shows three worked findings and fictional retest states. This pack explains the decisions and responsibilities needed to commission that kind of evidence.

[Open the SaaS and AI demonstration report](#)

Page	What to inspect
2	Worked scope and access boundaries
3	Report structure and example version record
4	Quality review and release conditions
5	Client handoff and retest expectations
6	Partner decisions and first project intake

Founder-led identifies delivery ownership. Independent identifies assessment separate from implementation. Disclose any implementation role and arrange appropriate independent review before describing resulting validation as independent assurance.

Worked Scope and Access Boundaries

ExampleSaaS Sandbox is a fictional two-tenant application with a support agent. A product agency coordinates the engagement; the client authorizes access; DevBrows owns the agreed assessment and technical report. This compact example is not a complete SaaS or AI test plan.

Scope item	Illustrative agreement
Purpose and recipient	An enterprise customer requests evidence about tenant data access and agent actions. Identify the buyer reviewer and confirm format, test coverage, permitted disclosure and tester qualifications before booking. Acceptance remains with that reviewer.
Environment	One staging web application and REST API at reserved .example addresses; synthetic records in tenants Alpha and Beta. Record exact routes, deployed build, model/provider, agent configuration, retrieval index and tool versions in the signed scope.
Identities	alpha_member, alpha_billing_admin, beta_member, agent_service, user_alpha_one and user_alpha_two. Client provisions these six controlled identities and confirms intended permissions.
Workflows	Report access and export; support retrieval and refund approval; private conversation memory. Plan role, tenant and user boundary checks, including a permitted control case and a denied case for each boundary.
Limits and exclusions	No production data, real payment movement, availability testing, social engineering, cloud infrastructure, mobile application, source review or foundation-model assessment. Record blocked checks; do not label them passed.
Approval and stop conditions	Written client authorization specifies exact targets, window, methods and contacts. Stop on unexpected sensitive data, instability or access beyond scope; notify the named escalation contact through the agreed channel.

Scope change rule

A new connector, additional tenant type, changed tool authority or different deployment requires an impact review. Record whether the change fits the agreement or requires revised scope, fee and dates before testing it.

A standalone SaaS scope would omit agent workflows. An AI scope must retain the relevant application, identity and tool boundaries. This combined example is not a price quotation.

Report Structure and Version Record

Agree the report structure with the partner and client before access. Preserve a technical report for engineering and a suitable evidence summary for approved procurement recipients; the summary must retain material limitations.

Section	Required content
Document control	Client and recipients, confidentiality, report version, assessment dates, named tester and reviewer, authorization reference, actual qualifications where relevant.
Executive summary	Reason for testing, important findings, business consequence, remediation priorities and remaining gaps. Explain that results apply to the tested scope and snapshot.
Scope and coverage	Assets, builds, roles, tenants, workflows, methods, exclusions and blocked tests. Each coverage row records expected boundary, result, evidence reference and limitations.
AI authority map	Caller, service and agent identities; delegated scopes; retrieval and memory access; tool operations; approval boundaries; model and tool versions. Include only where relevant.
Finding detail	Stable ID, affected asset, preconditions, reproduction steps, positive control, controlled evidence, impact, severity reasoning, proposed fix and fix owner.
Remediation and retest	Finding ID, supplied change reference, retest snapshot and date, cases attempted, observed result, remaining risk and explicit status. Attach a scoped addendum rather than erase the baseline.
Evidence and appendices	Evidence index, data handling, approved references, buyer summary and the limitations of scoring or framework mappings. Never imply full framework certification from selected checks.

Fictional version example

Record	Change and remaining limits
Baseline v1.0	B1 contains F01 cross-tenant report disclosure, F02 refund approval failure and F03 private-memory disclosure. All are constructed examples.
Retest addendum v1.1	B2: F01 fixed for stated cases; F02 partially fixed with expired approval still accepted; F03 not retested because memory was unavailable. None is a real result.

In a real report, dates, versions, personnel and evidence are recorded from the engagement. An unresolved issue stays visible until validation supports changing its status.

Quality Review and Release Conditions

These are proposed review steps to agree for each project. The proposal names a technically capable reviewer and records any limits on review independence. This public pack does not claim that a review has been performed.

Gate and owner	Checks and release condition
1 Scope readiness Delivery owner with client and partner	Confirm authorization, recipient requirements, available test identities, asset inventory, synthetic data, contacts, allowed tooling and stop conditions. Resolve scope gaps before access; confirm capacity before committing dates.
2 Technical evidence Named technical reviewer	Trace each finding to reproducible evidence, authorized identities, preconditions and the tested snapshot. Check the expected permitted case as well as the failed boundary. Remove scanner-only or unsupported conclusions.
3 Coverage and severity Reviewer with delivery owner	Reconcile findings with coverage rows. Distinguish observed behavior, hypotheses, blocked tests and exclusions. Check business consequence and severity assumptions. Supply a CVSS version and vector if agreed; do not invent scores.
4 Release and disclosure Delivery owner with approved recipients	Check redaction, links, references, report version and retest status. Record review comments and their resolution. Resolve blockers before release; agree any remaining limitations with the client and keep them visible.

Review record to retain

Record reviewer name and role, report version reviewed, review date, finding IDs checked, evidence references inspected, corrections requested, closure evidence and release decision. Keep the record with the controlled engagement materials.

Implementation and independence

Engineering advice and verification are distinct from implementing the change. If DevBrows implements fixes under a separate scope, disclose who implemented, tested and reviewed them. Arrange appropriate independent review before calling the resulting validation independent assurance.

The checklist is informed by OWASP reporting guidance and the CREST procurement and follow-up guide. Referencing them does not imply accreditation, membership or guaranteed buyer acceptance.

Client Handoff and Retest Expectations

Define the handoff in the proposal so a partner, engineering team and buyer know which materials they receive and who owns the next action. The times below are illustrative planning allowances, not published service commitments.

Stage	Material and responsibility
Before testing	Client approves the scope and report recipients; partner confirms relationship ownership and buyer requirements; DevBrows confirms technical fit, delivery owner, reviewer, dates and access readiness.
During testing	Agree progress cadence, channel and severity-based escalation before access. Send material findings privately to the named client contact with evidence and practical next steps; do not wait for the final PDF when escalation is required.
Report release	DevBrows provides the versioned technical report and approved evidence summary through the agreed secure channel. Partner coordinates recipients. Client confirms receipt and raises factual corrections; a correction remains linked to its report version.
Engineering workshop	Example allowance: one 60-minute walkthrough. Review evidence, fixes and regression cases; assign client engineering owners and target dates. Substantial implementation or additional workshops require explicit scope.
Scoped retest	Example allowance: one retest round requested within 30 calendar days of report release for agreed finding IDs in the agreed environment. Confirm access, build and fix references. Record status and residual risk; new assets or repeated rounds need a new agreement.
Buyer handoff and closeout	Example allowance: one 30-minute partner handoff. Share only client-approved materials; retain unresolved findings and coverage limits. Client removes access; DevBrows confirms agreed retention and deletion actions and records open follow-up.

Status language that preserves the limits

Fixed for tested cases: stated boundary checks succeeded on the recorded snapshot. **Partially fixed:** some cases improved, but a defined path remains. **Unresolved:** the observed issue persists. **Not retested:** no verification result is available. A client statement that a fix was deployed is not retest evidence.

The illustrative report uses all relevant distinctions: F01 fixed for specified cases, F02 partially fixed, and F03 not retested. A retest does not establish that the whole system is secure.

Partner Decisions and First Project Intake

Bring one qualified client project and the delivery gap it creates. Confirm these decisions before sharing engagement data or reserving capacity. The signed terms and scope govern each project.

Decision	What to agree
Client ownership	Referral: DevBrows contracts and delivers directly, with separately agreed referral terms. Co-delivery: identify the prime contractor, client contact permissions, communications owner and invoicing responsibilities.
Attribution and distribution	Agree report branding, tester and reviewer attribution, permitted recipients and who approves disclosure. Any white-label arrangement still requires client authorization and transparent delivery roles.
Commercial and scheduling	Set scope, fee, payment terms, tax treatment, dates, dependencies and change process in writing. Reserved capacity or volume terms follow confirmed demand and a reviewed first delivery; they are not assumed from an introduction.
Confidentiality and evidence	Agree NDA, access-controlled storage, secure transfer, recipient access, data location, retention and deletion. Third-party AI use with engagement data requires prior agreement. Do not send credentials or raw client data in an initial inquiry.
Risk and remediation ownership	Name client fix owners and the person who can accept residual business risk. DevBrows records evidence and verification limits; the buyer or auditor decides whether the report meets its requirements.

First project intake

Share the system and business requirement; web/API and AI workflow scope; intended buyer or auditor and required report format; deadline and budget range if known; expected project volume; current provider or delivery problems; and preferred referral or co-delivery model.

[Discuss a Security Partner project](#)

References for these planning checks

[OWASP WSTG v4.2 Reporting](#)

[CREST A Guide to Penetration Testing 2022](#)

[DevBrows methodology and engagement standards](#)