Client assurance pack.

What to expect before, during and after an engagement: sample deliverables, authorisation, rules of engagement, confidentiality, retention and destruction, and the assurance documents you can request.

This pack summarises how we work. The signed engagement documents govern. If anything here differs from those documents, the signed terms apply.

1. Sample deliverables

These are the documents a typical assessment produces. The exact set is agreed in the engagement terms; not every programme includes every item.

TYPICAL ENGAGEMENT DELIVERABLES

DELIVERABLE	WHAT IT CONTAINS
Scope and Rules of Engagement	Objectives, assets, access, stop points, authorised systems, personnel and testing windows.
Test plan and attack-path map	The routes, trust boundaries and tests we will run, agreed before testing begins.
Findings report	Validated findings with reproducible evidence, CVSS 4.0 severity, CWE, business impact and remediation.
Executive summary	A short decision brief for leaders: the risks that matter and the next actions.
Remediation tracker	Findings, owners, status and the result of each retest.
Retest record and evidence pack	The same tests replayed after the fix, with the result recorded.
Close-out note	What was tested, what changed, what remains and what the review could not prove.
Raw evidence	Available on request under the engagement terms.
Sample findings report	Download a fictional sample (PDF). It uses the same structure as a delivered report, with a fictional client, findings and retest record.

Deliverables are written for the people who own the system. Findings include the evidence needed to reproduce the result and the limits of what we tested.

2. Authorisation procedure

We only test what the system owner has approved in writing. The procedure is the same for every engagement.

Written authorisation from a named representative of the system owner.

Scope, assets, source addresses, personnel, testing windows and stop points agreed in writing.

No testing from an enquiry, a report or a website form. Passive observation of public information is the only exception.

Changes to scope, method or timing re-authorised in writing before they happen.

A named contact and stop procedure on both sides. Testing stops if the client asks.

Evidence handled under the confidentiality arrangements below.

Access removed at close-out.

A website statement, an enquiry or a vulnerability report is not permission to test.

---

3. Rules of engagement

Every assessment starts with written Rules of Engagement covering:

- Scope and Rules of Engagement
- NDA and confidentiality obligations
- Data handling and retention requirements
- Evidence and findings ownership
- Incident and breach notification procedures
- Authorised systems, personnel and testing windows
- Prohibited actions: denial of service, destructive testing, third-party systems, and social engineering unless explicitly approved
- Escalation and stop contacts

The signed Rules of Engagement govern. This list is a summary.

---

4. Confidentiality arrangements

Confidentiality and data handling are agreed before anyone gets access.

- A mutual NDA before access; the engagement terms add confidentiality and data-handling obligations.
- Need-to-know access and named personnel; access is removed at close-out.
- Encrypted storage and transfer; customer-managed keys where agreed.

- Evidence minimisation and redaction; synthetic data where the work allows it.
- No client data in public case studies or marketing without written approval.
- Sub-processors named and approved; we do not sell client data.
- Return or delete on request, or at the end of the retention period.

Our confidentiality and NDA terms are published in full. The signed mutual NDA and engagement documents govern.

5. Data retention and destruction

Client engagement data is kept for the period set in the signed engagement terms. We return or destroy it when that period ends.

RETENTION SCHEDULE

DATA	PRACTICE
Client engagement data	Retained for the period set in the signed engagement terms. We return or destroy it when that period ends, and confirm destruction in writing where the terms require.
Backups	Deleted on the rolling backup schedule; copies may remain in backups until they roll off.
Website enquiries and referrals	Kept for 12 months after the request closes.
Incident and vulnerability reports	Kept for 24 months after closure.
Email delivery records	Kept for 30 days.
Deletion requests	Actioned within 30 days unless a legal or security hold applies.

Website form data follows the privacy policy. Client engagement data follows the signed engagement terms, which take precedence for that engagement.

6. Assurance documents

We share current assurance documents on request. The trust centre shows what is available today, and we answer the auditor, scope and period for the specific document you need.

DOCUMENTS YOU CAN REQUEST

DOCUMENT	WHAT YOU RECEIVE
SOC 2 report	Available on request. You receive the report, the auditor, the scope and the period.
ISO 27001 certificate	Available on request. You receive the certificate, the certification body, the scope and the period.
Security questionnaire	Available on request. Send the topics and your deadline, and we will answer what the documents do not cover.
Client assurance pack	Published here and as a PDF. It summarises the signed engagement documents, which govern.

We do not publish the SOC 2 report or ISO 27001 certificate as open downloads because they contain control detail under confidentiality. Send the document list and your deadline in a supplier review.

7. Using this pack

Use this page for an initial review. The signed engagement documents are the authoritative record. If your review needs a specific document, a completed questionnaire or a call, tell us the topics and your deadline.

Contact hello@riftweld.com or start a supplier review.