

How we deliver, phase by phase

Every engagement moves through the same seven phases, from the first conversation to standing support. Each one shows the work, what you receive, your part in it, and how both sides know it is done: the same facts published on our service and trust pages, and what you can commit to an auditor before you sign.

Version 1.0 · August 2026. This document mirrors the methodology published at virtuestech.com/methodology/. If the page and this PDF ever disagree, the page is current.

The seven phases at a glance

A two-week assessment and a three-year program pass through the same phases; only the cadence changes. Pages 2 and 3 give the detail for each.

- 01 Discover** Understand the product, the release, and where failure hurts most.
- 02 Scope** Targets, rules of engagement, and evidence out, agreed in writing.
- 03 Engineer** Senior engineers run the work, with daily contact.
- 04 Validate** Findings demonstrated, ranked, and written to be acted on.
- 05 Retest** Fixes verified, the report updated.
- 06 Transfer knowledge** The capability becomes your team's.
- 07 Support** Repeat on your cadence, co-run, or hand over.

What this document is for. A versioned, dated copy of our published methodology for vendor files, procurement packs, and audit evidence. It is ungated, like the page it mirrors. Framework alignment and governance commitments are on page 4; company facts and the vendor due-diligence process are at virtuestech.com/trust/.

01 Discover Understand the product, the release, and where failure hurts most.

ACTIVITIES

A first conversation with the engineers who would deliver the work: your product, your architecture, and the deadline behind the request.

YOUR INVOLVEMENT

Bring the audit date, the security questionnaire, or the release plan. We work backwards from what you need to prove.

DELIVERABLES

A shared view of where failure hurts most, and of which evidence will satisfy the auditor, the customer, or the board that asked.

SUCCESS CRITERIA

Both sides can name the risk in play and the artifact that will settle it.

02 Scope Targets, rules of engagement, and evidence out, agreed in writing.

ACTIVITIES

A scoping call with the testers themselves. Targets, rules of engagement, and the evidence you need out are agreed in writing.

YOUR INVOLVEMENT

You set scope and sign the rules of engagement. The people on this call are the people who will run the work.

DELIVERABLES

Written scope, signed rules of engagement, agreed communication channels, and a mutual non-disclosure agreement before any testing begins.

SUCCESS CRITERIA

Everything the engagement depends on exists on paper before the first test runs.

03 Engineer Senior engineers run the work, with daily contact.

ACTIVITIES

Security testing runs manually, aligned to the OWASP Testing Guide, PTES, and NIST SP 800-115. Quality engineering runs risk-ranked test charters in time-boxed cycles.

YOUR INVOLVEMENT

Daily contact. Critical findings reach you the day they are demonstrated; nobody waits for the report to learn bad news.

DELIVERABLES

Defects triaged daily with clear severity calls, and automation built in your CI on frameworks your team already uses.

SUCCESS CRITERIA

The agreed scope is exercised in full and nothing urgent sits waiting in a draft report.

04 Validate Findings demonstrated, ranked, and written to be acted on.

ACTIVITIES

Every finding is demonstrated with reproduction steps and evidence of impact, then ranked by exploitability and impact rather than scanner scores.

YOUR INVOLVEMENT

You review each demonstrated finding with its evidence. Remediation guidance arrives ordered, so your team knows what to fix first.

DELIVERABLES

An executive summary your board can read and technical findings your engineers can act on without a follow-up meeting.

SUCCESS CRITERIA

Nothing in the report is theoretical. Anyone on your team can reproduce a finding from the steps written down.

05 Retest Fixes verified, the report updated.

ACTIVITIES

Your team fixes on its own schedule. We verify each fix on retest and update the report to “remediated and retested”, the phrase auditors look for.

YOUR INVOLVEMENT

Tell us when the fixes land. The retest checks them against the original reproduction steps.

DELIVERABLES

A retest-verified final report you can hand to auditors and enterprise customers as it stands.

SUCCESS CRITERIA

Remediation is verified rather than assumed, and the final report says so.

06 Transfer knowledge The capability becomes your team's.

ACTIVITIES

Handover documentation, pairing sessions, and, where the engagement calls for it, secure-coding workshops built around the findings from your own systems.

YOUR INVOLVEMENT

Your engineers pair with ours during handover, so the first person to maintain the work has already run it.

DELIVERABLES

The framework, the documentation, the CI integration, and a maintenance playbook. You own all of it.

SUCCESS CRITERIA

Handover is an explicit exit criterion: what we built keeps working after we leave.

07 Support Repeat on your cadence, co-run, or hand over.

ACTIVITIES

The cycle repeats on your release cadence, or we stay on as your managed team across testing, automation, or SOC coverage, under the same governance either way.

YOUR INVOLVEMENT

You choose the shape: run by us, co-run with your team, or handed over entirely once it is self-sustaining.

DELIVERABLES

Evidence that stays current: refreshed reports each cycle, regression packs that grow with every finding, and detection content built from what testing proved exploitable.

SUCCESS CRITERIA

Next quarter's questionnaire meets this quarter's report.

Cadence, not content, is what changes. A two-week assessment and a three-year program pass through the same phases. Recurring programs repeat phases 3 through 5 each cycle under the scope and governance agreed once in phases 1 and 2.

The frameworks the work maps to

Penetration testing & security testing

Testing is aligned to the OWASP Testing Guide, PTES, and NIST SP 800-115, with retest included as standard: remediation is verified on retest and the report updated to “remediated and retested.”

Quality engineering

Requirement-traced test design ranked by risk, executed with disciplined evidence capture. Where accessibility is in scope, work is assessed against WCAG 2.2 AA, EN 301 549, and Section 508.

How every engagement is governed

Under NDA

Every engagement runs under a mutual non-disclosure agreement. Scope, rules of engagement, and communication channels are agreed before any testing begins.

Methodology & retest

Testing is aligned to the OWASP Testing Guide, PTES, and NIST SP 800-115. Remediation is verified on retest and the report updated to “remediated and retested.”

Personnel security

Engineers who handle client data sign NDAs and undergo background checks. The people who scope your engagement are the people who run it. No anonymous offshore bench.

Data handling

Findings and reports are shared only through the channels agreed at scoping and retained only for the period needed to deliver and support the engagement. Storage, encryption, retention, and destruction specifics are set in your service agreement.

Verifying this document. Company facts, certifications held by our engineers, and the vendor due-diligence process are published at virtuestech.com/trust/. The evidence behind every claim on our site, including this methodology, is published row by row at virtuestech.com/evidence-register/. A redacted sample penetration-test report is a direct download at virtuestech.com, no form required.