OVERVIEW

WS02
2–3 weeks
Forge Honor Assurance

SBA U.S. Small Business Administration
VETERAN-OWNED CERTIFIED

Vendor Security Readiness Review

Representative sample engagement for a web application and API security review.

ENGAGEMENT FIT

Software teams preparing for procurement, enterprise customer review, or board-facing security questions.

SCENARIO

A small SaaS team is about to enter a vendor security review with an enterprise customer. The product has a React front end, API services, cloud deployment, third-party authentication, and customer-specific data access. The team needs a credible report and a prioritized remediation plan.

CONSTRAINTS

- The review must avoid disruption to production users.
- The buyer needs written evidence suitable for customer security teams, but not a formal compliance certification.
- Engineering time is limited, so findings must be prioritized by business risk and fix effort.
- Access is scoped to a repository snapshot, staging environment, architecture notes, and selected configuration evidence.

This is a representative composite report showing the type of work product Forge Honor Assurance can provide. It is not a client case study.

REPORT DATA

SAMPLE ID
WS02

CATEGORY
Security Audit & Code Review

TIMEFRAME
2-3 weeks

BEST FOR
Software teams preparing for procurement, enterprise customer review, or board-facing security questions.

USE NOTE

Representative composite sample. No client PII, proprietary environment detail, or confidential facts are included.

Final scopes, controls, deliverables, and timelines are confirmed in writing per engagement.

Scope and Delivery Plan

A practical work plan with written scope, explicit boundaries, and deliverables the buyer can inspect.

SCOPE

- Review authentication, authorization, session handling, and customer data separation paths.
- Inspect sensitive data handling, logging, dependency posture, environment configuration, and secrets patterns.
- Exercise representative workflows in staging where authorized.
- Produce findings with severity, evidence, likely impact, remediation guidance, and retest criteria.
- Package an executive summary and remediation roadmap.

TIMELINE

PHASE	FOCUS	EXPECTED WORK
Day 0–1	Scope and access	Confirm systems in scope, testing rules, repo/environment access, and report audience.
Days 2–5	Code and config review	Inspect auth, data access, logging, dependency posture, CI/CD, and deployment configuration.
Days 6–8	Manual validation	Reproduce selected issues in staging and collect evidence without touching production data.
Days 9–10	Report drafting	Write executive summary, findings, remediation plan, and retest checklist.
Optional week 3	Fix support and retest	Pair with engineers or review patches, then issue a verification memo.

DELIVERABLES

- **Executive summary: Plain-language risk posture, themes, and priority recommendations.**
- **Findings report: Each finding includes severity, evidence, impact, fix guidance, and retest criteria.**
- **Risk register: Sortable list by severity, affected area, owner, effort, and target closure date.**
- **Remediation plan: What to fix this week, this month, and what to defer with a documented rationale.**
- **Verification memo: Optional short memo after retest for customer or leadership review.**

SAMPLE OUTPUT

WS02
2–3 weeks
Forge Honor Assurance

Sample finding format

Findings are written so engineers can close them and non-engineers can understand why they matter.

FIELD	EXAMPLE
Finding	Tenant object access relies on client-supplied organization identifier.
Severity	High - possible cross-tenant data exposure if authorization checks are bypassed.
Evidence	API request accepted an orgId parameter not derived from the authenticated session.
Remediation	Resolve tenant context server-side from the session and add authorization tests for cross-tenant requests.
Retest	Requests for another tenant's object return 403 and are logged with no data in response body.

HANDOFF

- **The buyer receives a written report, prioritized closure plan, and a realistic path to customer-facing evidence.**
- **If remediation support is included, changes can be paired, reviewed, or implemented directly depending on repo access.**
- **The final retest memo is concise enough to share with customers, primes, or leadership.**

Sample remediation priority

A useful report separates urgent fixes from cleanup that can be scheduled after the critical path.

PRIORITY	THEME	ACTION
P0	Authorization	Patch tenant context issue and add regression tests.
P1	Secrets	Rotate exposed staging secret and move config to managed secret store.
P1	Logging	Remove sensitive request payload fields from application logs.
P2	Dependencies	Upgrade vulnerable transitive package and pin review cadence.

BOUNDARIES

- **This is not a formal penetration test unless explicitly scoped that way.**
- **This is not SOC 2, ISO, FedRAMP, or legal compliance certification.**
- **Testing is limited to authorized systems, environments, and time windows.**