GRC+ SERVICE SHEET · NOVEMBER 2026

Source Code Review

Some flaws are far easier to find in the code than from outside. We run static analysis to cover the whole codebase, then read the security-critical parts by hand, and show your developers exactly what to change.

SERVICE
Advisory service

USUALLY TAKES
Days to weeks, depending on the size of the code base

What It Is

Security reviews of your source code by experienced reviewers, checked against OWASP ASVS, with each finding located in the code and a fix.

WHY IT MATTERS
Scanners find patterns, not intent
Static tools produce a lot of noise and miss flaws in the logic of your application.
- False positives that waste developer time
- Logic flaws no tool sees
- Secrets and unsafe defaults in code

THE OUTCOME
Fixes where your developers work
Each finding names the file and line, and shows how to fix it.
- File and line for each finding
- Fix examples
- A walkthrough with your developers

What We Test

Who you are and what you can do	Authentication, authorisation, access control and session handling.
Data handling	Input validation, sanitising, data access, encryption and error handling.
Runtime behaviour	Memory and resource handling, logging and what is written to it.
Dependencies	Third-party libraries and how they are used.
DevSecOps	A maturity assessment of your CI/CD pipeline and DevOps practice against OWASP SAMM, with hands-on checks of the components that carry the most risk.

What You Receive

The code review report PDF	Each finding with its evidence, risk, the steps to reproduce it and a fix.
A management summary In the report	What was tested, the main risks and the decisions needed, without the technical detail.
A walkthrough Video call	A session with your team to go through the findings and answer questions.
A retest on request Updated report	We check your fixes and update the report, so you can show the result to auditors and customers.

From Scope to Verified Fixes

1	**Scoping** Targets, people, test windows and exclusions, with written authorisation and rules of engagement.
2	**Automation** Static analysis of the code, with custom searches where they help.
3	**Review** Results validated, then security-critical code read by hand.
4	**Report** Findings with evidence, risk and a fix, a management summary and a walkthrough with your team.
5	**Retest** We check your fixes and update the report.

A guide, not a fixed promise: the length of each phase depends on your scope.

Regulations That Ask for It

CRA	Security reviews of your source code by experienced reviewers, checked against OWASP ASVS, with each finding located in the code and a fix.
RED DA	
IEC 62351	
ED-202A / DO-326A	
ISO 24089	
GSMA NESAS	
ETSI EN 303 645	
IEC 81001-5-1	
FDA 524B (United States)	
NIST SSDF	
PLD	
CRA Product Categories	A review of your product code against the CRA essential cybersecurity requirements before conformity assessment.

Why Organisations Choose GRC+

Independent of your suppliers	We test what you have. We take no margin on a product we assess or recommend.
Findings tied to your requirements	Our team also works on NIS2, DORA, ISO 27001, PCI DSS and Swift CSP, so results can serve your audits too.
Risk rated for your business	We rate each finding by what it could cost you, not only by a scanner's score.
Written rules of engagement first	Scope, limits and contacts are agreed in writing before any test starts.

Questions Buyers Ask

Do you need access to our repository?

We need read access to the code in scope, in your environment or through a secure transfer. We agree the access method and how the code is handled before the review starts.

Should we choose a code review or a penetration test?

They complement each other. A code review finds flaws in how the code is written; a penetration test shows how the running system can be attacked. For critical applications we recommend both.

Which languages do you review?

Tell us your languages and frameworks when you ask for a proposal. We confirm before we start that the reviewers on your project work with them.

Will this slow our developers down?

The aim is the opposite: checks that run on their own and only stop a release for what really matters. We review how the tools fit your teams as well as whether they are present.

Talk to Us

Thirty minutes with a principal consultant on what applies to you and what to do first.
Book a 30-Minute Call · sales@grc.plus · grc.plus/service/source-code-review

