GRC+ SERVICE SHEET · NOVEMBER 2026

Penetration Testing

We attack your applications, networks and cloud environments the way a real attacker would, within a scope and rules of engagement you agree first. You get each finding with its evidence, its risk and a fix.

SERVICE
Advisory service

USUALLY TAKES
Days to weeks, depending on scope, from kick-off to report

What It Is

Manual penetration tests of applications, APIs, networks and Wi-Fi, plus vulnerability assessment, host hardening and OSINT, with risk-rated findings and a practical fix for each.

WHY IT MATTERS

A scanner is not a test

Automated tools find known issues. They miss business logic flaws and chains of small weaknesses, and fill reports with false positives.

THE OUTCOME

A short list of real problems

You know what an attacker could do, what to fix first and how, and a retest shows auditors the fix works.

What We Test

Applications and APIs	Web applications, APIs, mobile apps and desktop clients, with and without a login.
Networks	Your internet-facing perimeter, and what an attacker could reach from inside your network.
Cloud and containers	Cloud accounts and Kubernetes platforms: permissions, exposure and configuration.
Combined scopes	One test across several target types, with one report and one point of contact.
Web and API	Manual testing of your web applications and APIs against the OWASP guides, with and without a login, with each finding verified and a fix for each.
Mobile	Android and iOS app testing against the OWASP Mobile Application Security guide: data on the device, app code, traffic and the APIs behind it.
Desktop App	Security testing of installed desktop and thick-client applications: the executable and its libraries, local permissions and the traffic to the backend.
Network	External and internal network tests that show what an attacker could reach and how far they could get, following NIST SP 800-115 and PTES.
Wireless Security	A test of your guest and corporate Wi-Fi: whether a visitor can reach your internal network, how strong your encryption is and how your network is separated.
OSINT	What attackers can already learn about your organisation from public sources: leaked credentials, exposed code, forgotten systems and staff details.
Vulnerability	External and internal scanning validated by hand, so you get a list of real vulnerabilities in priority order without false positives.
Hardening	A review of your server, workstation and database configuration against CIS Benchmarks or your own baselines, with authenticated scanning and validated results.

What You Get

The test 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, user roles, test windows and exclusions, with written authorisation and rules of engagement.	
2	**Testing** Automated and manual testing in the agreed windows. A critical finding is reported to your contact the same day.	
3	**Report and walkthrough** Findings with evidence, risk and a fix, a management summary and a session with your team.	
4	**Retest** We check your fixes and update the report, so you can show the result to auditors and customers.	on request

Regulations That Ask for It

PCI DSS	**Penetration testing for PCI DSS 11.4** Internal and external penetration tests of the CDE and its segmentation, with retests of the weaknesses you fix.
TM-E-1 (Hong Kong)	Annual penetration tests of Internet and mobile banking by an independent party, as section 3.3.2 requires.
QCB Technology Risks (Qatar)	Vulnerability assessments and penetration tests of your infrastructure and applications as section 9.4 requires.
CRA	Manual penetration tests of applications, APIs, networks and cloud environments, with risk-rated findings and a practical fix for each.
UN R155 / R156	
MDR	
RED DA	
ISO/SAE 21434	
Cybersecurity Act	
eIDAS 2	
Safeguards Rule (United States)	
MAS TRM (Singapore)	

Why 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

How often should we run a penetration test?

At least once a year and after significant changes, such as a new application or a major release. Some frameworks and contracts set their own frequency.

Do you test production systems?

Where you agree. Many tests run on a production-like test environment; tests on production use agreed windows and safe techniques.

Which standards do you follow?

Recognised methods, including the OWASP Web Security Testing Guide for web applications and NIST SP 800-115 for technical security testing, with findings rated on a common risk scale.

Which kind of penetration test do we need?

Start from what worries you or what your customer or regulator asks for. An internet-facing application points to a web test, a concern about ransomware to an internal network test. We help you choose on the first call.

Talk to Us

In 30 minutes you learn what is in scope, how we would approach it and what drives the fee. A written proposal follows within two working days.
Book a 30-Minute Call · sales@grc.plus · grc.plus/service/penetration-testing

