The SMB Pentest Readiness Checklist

Everything you need to prepare for your first penetration test, and the questions to ask any vendor (including us) before you commit.

CyberGuards · https://cyberguards.ai

Section 1 — Do you actually need a pentest right now?

A plain-language test. If any of these are true for your team in the next few months, the answer is probably yes.

- A customer's procurement or security team has asked for a current penetration test report.
- You have a SOC 2, ISO 27001, PCI DSS, or HIPAA audit on the calendar and the control list includes a periodic pentest as evidence.
- You had a security event — even a small one — and you want to know what else an attacker would have reached if the path had continued.
- You are moving upmarket and your next tier of customers signs in procurement, not in product.
- Your board or investors have asked for a defensible answer on what has been tested and what has been fixed.

If none of these apply, a pentest is probably premature. Start with a security baseline and revisit when the first trigger lands.

Section 2 — What to gather before the scoping call

- In-scope applications, APIs, and cloud accounts. A short list of what faces customers and what processes their data.
- Number of user roles and trust levels. Anonymous, authenticated user, admin, super-admin, machine-to-machine, support, etc.
- Hosting environment and access mechanism. Cloud provider, regions, how the tester reaches the environment (VPN, bastion, read-only IAM).
- Known risk areas you'd like specifically covered. Recent changes, third-party integrations you don't fully trust, anything that worries you at 2am.
- Compliance framework if one is driving the test. SOC 2, ISO 27001, PCI DSS, HIPAA — or none yet, which is also a valid answer.
- Deadlines that matter. Customer audit date, board meeting, certification window, fundraise milestone.

Section 3 — Five questions to ask any pentest vendor

1. Who actually runs the engagement — and what's their certification level? You want a name and a track record, not "our team".
2. Is a retest of reported findings included or extra? "Extra" answers become surprise change orders after the report ships.
3. What does the report look like? Can you show a sanitized sample? If the vendor cannot share one, assume the format is the auditor-only PDF you don't actually want.
4. How do you handle a critical finding mid-engagement? You want a same-day disclosure path, not "in the final report."
5. What's the scope agreement and rules-of-engagement process? Written scope, written rules, signed before any traffic touches your systems.

Section 4 — How to read a pentest report without an engineering degree

- The board summary. One short paragraph that answers: was anything critical found, what was tested, and what was fixed. If the report does not lead with this, the report is hiding from you.
- Severity ratings. Critical / High / Medium / Low are not absolute — they are the vendor's recommendation for which findings to fix first. Sort by business impact in addition to the rating.
- The proof-of-concept and why it matters. Each finding should include the exact steps and evidence that prove the issue is real. Without a working proof, a finding is a guess.
- The remediation. The fix should be specific enough for an engineer to paste into a ticket. "Use defense in depth" is not a remediation.
- The retest section. The final report should reflect the post-fix state, not the test-day state. If your retest is not in the report, ask for it before sharing the report with auditors or customers.

Section 5 — After the test

The report is the start, not the end. Three things to plan for:

- Triage and prioritization. Sort findings by business impact, not only by CVSS. A medium-severity flaw in your payment path may be more urgent than a critical-severity flaw in an internal admin tool.
- Communicating findings to customers and auditors. Most pentest reports can be shared as-is under NDA. The board summary and control mapping are usually what auditors and procurement actually read.
- What to share publicly and what to keep internal. Specific exploit details and unfixed vulnerabilities stay internal. Aggregate posture (e.g., "annual third-party pentest, latest report dated X") is appropriate for a security page or trust portal.
- Re-testing cadence. Annual is the baseline. After every major architecture change or new product line is a fair addition. After acquisitions or significant team turnover, also worth scheduling.

Want to talk to the people who'd test you?

Book a 30-minute scoping call.

https://cyberguards.ai/contact/