

Pen test control map

What your reviewer asks for, and what a Snipeyes penetration test report provides.

DECISION SUMMARY

1. Agree method, scope, frequency and retest with your tester before the test starts.
2. Ask for findings mapped to the controls your reviewer will check.
3. Keep the report, the retest result and the test dates together in one audit file.

Framework and control	What the auditor asks for	What a Snipeyes report provides
PCI DSS PCI DSS v4.0.1 11.4.1	A documented penetration testing methodology based on industry-accepted approaches, covering the cardholder data environment perimeter and critical systems, testing from inside and outside the network, application-layer and network-layer testing, and retained results	Every finding proven; findings mapped to PCI DSS 4.0; one report with a leadership summary and engineer detail
PCI DSS v4.0.1 11.4.2 and 11.4.3	Internal and external testing per the defined methodology, at least every 12 months and after significant change, by a qualified tester with organizational independence	Findings mapped to PCI DSS 4.0
PCI DSS v4.0.1 11.4.4	Exploitable findings are corrected, and testing is repeated to verify the corrections	Every finding proven. Retest included.
PCI DSS v4.0.1 11.4.5	If segmentation isolates the cardholder data environment: tested at least every 12 months and after changes to it	Findings mapped to PCI DSS 4.0
ISO/IEC 27001:2022 ISO/IEC 27001:2022 Annex A 8.8 "Management of technical vulnerabilities"	Information on technical vulnerabilities is obtained, exposure is evaluated and appropriate measures are taken. ISO/IEC 27001 sets no test type or cadence; your risk assessment does	Findings mapped to ISO/IEC 27001:2022
ISO/IEC 27001:2022 Annex A 8.29 "Security testing in development and acceptance"	Security testing processes are defined and implemented in the development life cycle	Findings mapped to ISO/IEC 27001:2022 and OWASP ASVS
SOC 2 SOC 2 CC4.1 (monitoring, separate evaluations)	Penetration testing is listed among example separate evaluations. Points of focus are illustrative; no fixed frequency	Findings mapped to SOC 2
NIST CSF 2.0 NIST CSF 2.0 (Function level)	Six Functions: Govern, Identify, Protect, Detect, Respond, Recover (released February 26, 2024). A leadership-level frame, not a testing requirement	One report with a leadership summary
REGIONAL REGULATORS MAS Technology Risk Management Guidelines (January 2021), 13.2	For internet-facing systems, testing at least once annually or after major changes or updates	Findings mapped to the regulator's rules
APRA CPS 234	Testing by appropriately skilled and functionally independent specialists (CPG 234, guidance, names penetration testing)	Findings mapped to the regulator's rules

Report within 10 business days of testing.

Snipeyes provides the testing and the evidence. Your assessor or certification body decides what is accepted.

CREST Member. Certified to ISO/IEC 27001:2022.

Book a free 90-minute scoping session: calendly.com/snipeyes. Request a scoped proposal: snipeyes.com/request-order. Contact sales@snipeyes.com.

Reflects PCI DSS v4.0.1 and public sources checked 2026-10-10.

