

GUIDE

Reading a penetration test as a director

What a penetration test is, what to look for in the summary the board receives, and five questions that make it useful.

Current as of October 13, 2026 · 3 minute read

A penetration test is one of the few pieces of independent evidence a board receives about cybersecurity. Testers act like real attackers and try to get past the institution's defenses. NIST describes it as mimicking real-world attacks to find ways around the security of a system or network.

It is not the same as a vulnerability scan. A scanner reports that a weakness might exist; a penetration test tries to use it, to prove that it does. That is why a good test is worth reading closely.

What the examiners expect

- How often, and how deep, should follow the level of assurance the institution needs, and increase when systems, networks or threats change (FFIEC Information Security booklet, IV.A.1 and IV.A.2).
- Testers should be independent of what they test: not the people who designed or installed it (IV.A.3).
- Reports should rank findings by importance, suggest fixes and point out repeat issues; summary reports should be made available to the board as appropriate (IV.A.4).
- Findings should be tracked until the underlying weakness is fixed (IV.A.2).

What to look for in the summary

- Scope, and what was left out. A clean result on a narrow scope says little about the rest.
- Severity. Most reports use CVSS: Low 0.1 to 3.9, Medium 4.0 to 6.9, High 7.0 to 8.9, Critical 9.0 to 10.0. CVSS measures how severe a weakness is, not what it would cost your institution.
- Repeats. A finding that appeared in the last test too is a management question, not a technical one.
- Age. How long each critical and high finding has been open, against the remediation window in your own policy.
- Retest. Evidence that fixed findings were tested again, not only marked closed.

Five questions to ask

- 1 Who chose and engaged the testing firm, and does it report to the board or committee as well as to management?
- 2 What was out of scope, and why?
- 3 Which findings repeat from the previous test?
- 4 Which critical and high findings are past the date our policy sets, and when will each close?
- 5 Have the fixes been retested?

BoardAlign reads your test reports against what the board was told about them, and shows severity, age and repeats where the board can see them.

Scope exclusions, remediation dates and retest evidence are recommended practice; the FFIEC text covers ranking, repeats, independence and tracking to closure.

Sources

FFIEC IT Examination Handbook, Information Security (2016), section IV.A. <https://ithandbook.ffiec.gov/>

NIST SP 800-115, Technical Guide to Information Security Testing and Assessment.

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>

FIRST, CVSS v4.0 specification. <https://www.first.org/cvss/specification-document>

General information for directors, not legal advice. Current as of October 13, 2026. Rules change: check the cited source before relying on it.