

GUIDE

What a good cyber report to the board looks like

One page the board can read in a meeting: what it should contain, how often it should arrive, and the signs it is not doing its job.

Current as of October 13, 2026 · 3 minute read

Most board cyber reports are accurate. The problem is that they describe activity rather than position: patches applied, training completed, tools deployed. A board needs to know something different: are we inside the limits we set, what changed, and what do you need from us.

The rules set the floor: a report to the board at least once a year on the program's status and its material matters. Recognized practice goes further. The 2026 edition of the NACD and ISA Director's Handbook on Cyber-Risk Oversight recommends reporting at least quarterly, and after any material incident or major change, with escalation thresholds agreed in advance.

A one-page layout that works

- 1 Position against appetite: where the institution stands against the limits the board approved, in a sentence.
- 2 What changed since the last report: new risks, closed risks, incidents, major projects.
- 3 Top risks: three to five, each with an owner, a status and the date it is expected to change.
- 4 Measures against limits: each figure beside the board's own limit, marked inside or outside it.
- 5 Testing: findings by severity, how long the critical and high ones have been open, and any that repeat.
- 6 Third parties: the critical providers, any incidents involving them, and reviews due.
- 7 Incidents: anything that met the notification threshold, and anything close to it.
- 8 Decisions or direction needed from the board.

Measures worth asking for

The NACD handbook suggests measures such as these. Each is more useful with a board-approved limit beside it and last quarter's figure for comparison.

- number and severity of incidents;
- time to detect and time to contain;
- patch compliance for critical systems, against the window in your own policy;
- concentration of risk in third parties, and the share of critical vendors assessed;
- training completion and phishing test results.

Signs the report is not doing its job

- It reads the same every quarter.
- It has no prior-period comparison.
- Figures differ from the fraud or BSA/AML report for the same events.
- Testing is reported as "complete" without severity or remediation dates.
- The board has never been asked for a decision.

A schedule helps

What a board should receive, and how often, is easier to check against a written schedule: annual items such as program approval and the independent test, quarterly measures, and immediate notice of material incidents. Our Board Cyber Scorecard and Schedule, by Mark Blazek, sets one out, and it is free on this site.

BoardAlign compares what your board has been told with what it should receive and how often, report by report, and shows the gaps.

Sources

12 CFR Part 748, Appendix A, III.F.

<https://www.ecfr.gov/current/title-12/chapter-VII/subchapter-A/part-748/appendix-Appendix%20A%20to%20Part%20748>

NACD and ISA, Director's Handbook on Cyber-Risk Oversight (2026).

https://www.nacdonline.org/globalassets/public-pdfs/2026_directors-handbook-cyber-risk_print.pdf

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

NIST Cybersecurity Framework 2.0 (2024).

<https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework>

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