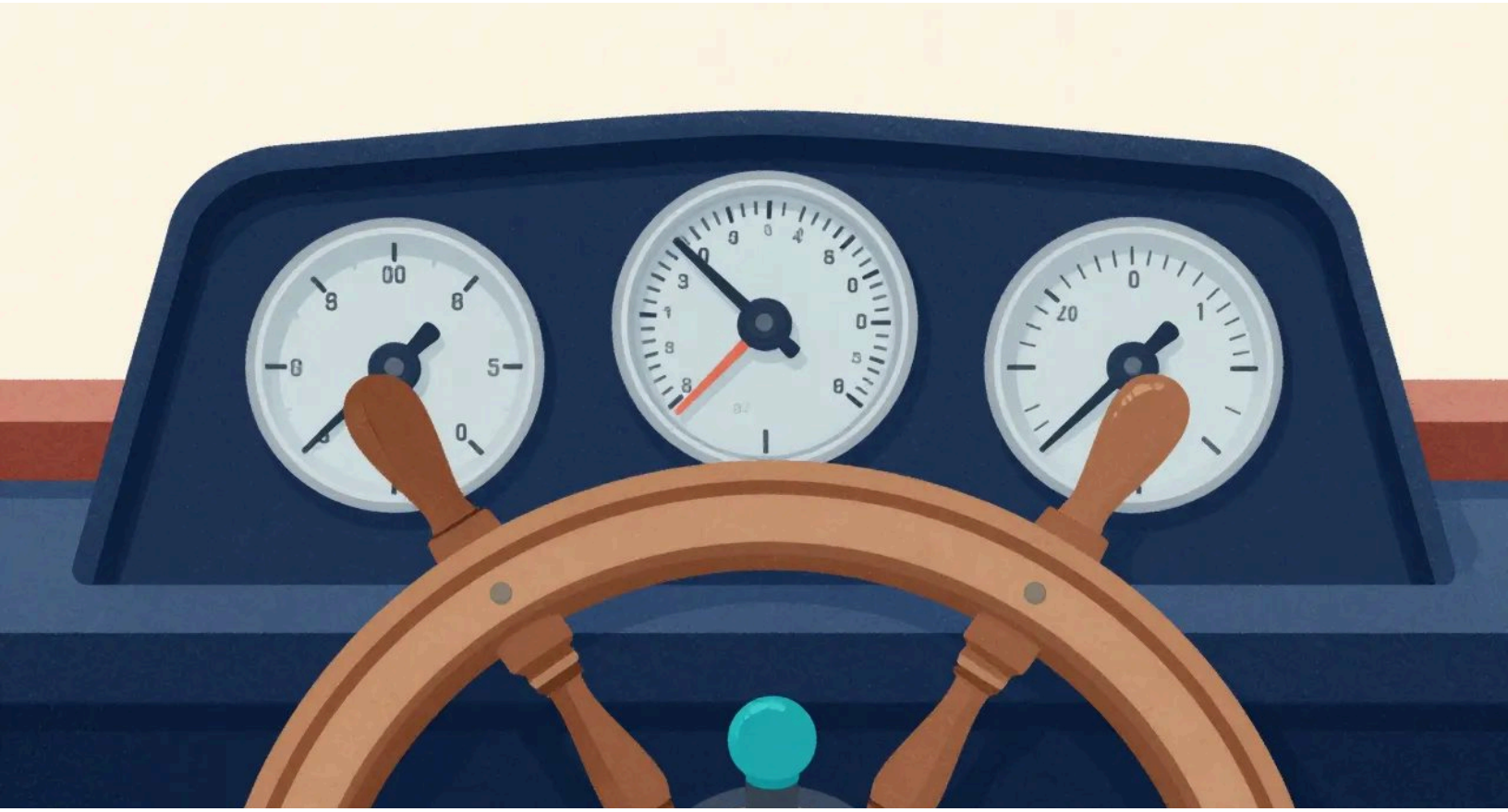


EXECUTIVE PAPER · INFRASTRUCTURE

# What the Board Should See Every Quarter

Boards are now accountable in law and in disclosure for technology risk, yet most still receive slide decks and tool screenshots that change every meeting. A fixed quarterly report of six measures, each with a target and a trend, gives directors something they can oversee.

AUTHOR

Chris Watkins

SERVICE

Infrastructure

FOR

CEO, Board · 11 min read

AT A GLANCE

**The problem.** Public companies must now describe in their annual report how the board oversees cyber risk. In the EU, financial firms' management bodies carry ultimate responsibility for ICT risk by regulation. Yet in a 2025 Gartner survey only 10% of non-executive directors were strongly confident their company had the right balance of protection and cost.

**Why it persists.** Technology updates reach the board as presentations built for that meeting. The measures change, the targets are missing, and last quarter's numbers are rarely shown beside this quarter's. Directors cannot see a trend in material that has no history.

**The recommendation.** Agree on six measures once, and report them every quarter in the same format with a target, an owner and four quarters of history: restore test results, exploited vulnerabilities on exposed systems, critical vendor concentration, change failure rate, recovery targets met, and AI systems in production with named owners. Spend board time on the measures that missed.

## The Decision in Front of You

The board already spends time on technology. The decision is what form that time takes. Most companies give directors a briefing from the CIO or CISO a few times a year, built fresh for each meeting, often with screenshots from a security tool or a list of projects. The alternative is a fixed report: the same small set of measures every quarter, each with a target the board approved, an executive who owns it, and a trend line.

The stakes are now legal as well as operational. Since fiscal years ending on or after December 15, 2023, United States public companies must describe in Form 10-K how the board oversees risks from cybersecurity threats, which committee is responsible, and how it is informed about those risks [1]. Material incidents must be disclosed on Form 8-K, generally within four business days of the company deciding they are material [1]. Whatever the board receives becomes the evidence behind those statements.

Most large companies say they report regularly. EY's review of 80 Fortune 100 companies that filed by July 31, 2025 found that 99% included language about how often management reports to the board on cybersecurity, but only 60% gave a frequency of at least annual or quarterly; the rest used words such as "regularly" or "periodically" [2]. On AI, 48% cited AI risk as part of the board's risk oversight, while only 16% described management reporting to the board on AI [2].

# What's Happening

## Directors are being asked to judge what they cannot measure

Gartner surveyed 330 non-executive directors between April 14 and May 22, 2025 [3]. Ninety percent lacked a measure of confidence in the value of cybersecurity spending, and 10% expressed strong confidence that their company had the right balance of protection and cost [3]. Gartner's advice was to report actual exposure and readiness instead of general threat trends and dashboards that confuse boards [3].

The National Association of Corporate Directors makes the same point in its 2026 Director's Handbook on Cyber-Risk Oversight. One of its six principles is that boards should guide cyber-risk measurement and reporting, with reporting that is structured, aligned with the business, and that translates technical metrics into financial terms [4].

## The frameworks now name the board's job

NIST's Cybersecurity Framework 2.0, published in 2024, added a Govern function. It says organizational leadership is responsible and accountable for cybersecurity risk (GV.RR-01) and that the results of risk management are reviewed to adjust strategy (GV.OV-01 to GV.OV-03) [5]. It also lists the controls the six measures below draw on: suppliers known and prioritized by criticality (GV.SC-04), backups created, protected, maintained and tested (PR.DS-11), and the integrity of backups verified before use in recovery (RC.RP-03) [5].

In the European Union, the Digital Operational Resilience Act, Regulation (EU) 2022/2554, has applied to banks, insurers, investment firms and other financial entities since January 17, 2025 [6]. Article 5 says the management body bears ultimate responsibility for managing the firm's ICT risk [7]. It must approve and periodically review the business continuity policy and the response and recovery plans, approve the policy on third-party ICT providers, and set up reporting channels that keep it informed about those arrangements and about major incidents [7]. Members must keep their knowledge current through regular training [7].

## Two cases show where the board's view and reality part

**SEC disclosure cases, October 2024.** The SEC settled charges against four technology companies that had been affected by the SolarWinds Orion compromise [8]. Unisys paid $4 million after describing cyber risks as hypothetical when it had already suffered two intrusions involving data exfiltration [8]. Avaya paid $1 million for describing access as limited to some email messages when it knew at least 145 files had also been accessed [8]. Check Point and Mimecast paid $995,000 and $990,000 [8]. The SEC's case against SolarWinds itself ended differently: a court dismissed most claims in July 2024, and the SEC dropped the rest with prejudice in November 2025 [9]. The lesson for directors is the narrower one the four settlements share. What the company tells investors must match what management knows, and the board can only check that if it receives the facts in a consistent form.

**Clorox and its service desk, 2023 attack, 2025 lawsuit.** In July 2025 Clorox sued Cognizant, its IT service desk provider, for $380 million [10]. Clorox alleges that on August 11, 2023 an attacker called the service desk, posed as an employee, and had passwords and multifactor authentication reset without the identity checks Clorox's procedures required [10]. Clorox says it took systems offline, paused manufacturing and processed orders by hand for weeks [10]. Cognizant disputes the claims and says it was hired for a narrow help desk scope [10]. Whoever prevails, the case shows that a vendor with the power to reset credentials is a critical vendor. A board that tracks only spend by supplier would not have seen it.

## Why the Usual Approach Fails

Board technology briefings are usually written for the meeting at hand. The presenter chooses what to show. A quarter with good news shows a maturity score; a quarter after an incident shows the incident. The measures change, so nothing can be compared across quarters, and directors fall back on judging the presenter.

Tool dashboards do not solve this. A vulnerability scanner reports thousands of findings, most never exploited. A count of blocked attacks says something about the internet and little about the company. These numbers rise and fall for reasons unrelated to the company's exposure, and directors cannot tell which movement matters.

A third problem is missing targets. A number without a target cannot be over or under. When a board sees "212 critical vulnerabilities," it has no way to know whether that is good, and the conversation turns to explanation instead of decision.

## The Framework: The Six-Line Report

The Six-Line Report gives the board one page each quarter with six rows. Each row has a definition fixed for at least a year, a target the board approved, an executive owner, and the last four quarters of results. Management may add commentary. It may not change the definitions without board approval.

**Exhibit 1. Six measures cover recovery, exposure, dependency, change and AI**

| Measure | What is counted | Example target | Owner | Anchor |
|---|---|---|---|---|
| Restore tests passed | Share of tier-one systems restored from backup in a test this quarter, within their approved recovery time | 100% of tier-one systems tested each year; at least 25% each quarter | CIO | NIST CSF 2.0 PR.DS-11, RC.RP-03 [5] |
| Exploited vulnerabilities on exposed systems | Flaws on CISA's Known Exploited Vulnerabilities list open on internet-facing systems, and the oldest one's age in days | Zero open longer than the published fix deadline | CISO | CISA KEV catalog [11] |
| Critical vendor concentration | Critical business functions that depend on one vendor with no tested alternative or exit plan; vendors that can reset credentials or reach production | Count falls each quarter; every such vendor reviewed yearly | COO with CISO | CSF 2.0 GV.SC-04 [5]; DORA Article 5 [7] |
| Change failure rate | Share of production changes to tier-one services that needed immediate intervention, such as a rollback or emergency fix | Trend shown; a threshold triggers review | CTO | DORA research metrics [12] |
| Recovery targets met | Share of real incidents and recovery tests this quarter where the approved recovery time and data-loss limits were met | 100%, with each miss explained | CIO | DORA Article 5(2)(e) [7] |
| AI systems in production | AI systems and agents in use, each with a named business owner, its data access, and date of last evaluation | Every system has an owner and an evaluation in the last two quarters | Executive sponsor for AI | NIST AI RMF, GOVERN 1.6 [13][14] |

Source: author's framework; anchors from the cited standards and regulations.

**Restore tests passed.** A backup that has not been restored is a claim. This row counts restores that worked, within the recovery time the business approved. Untested systems count as failures.

**Exploited vulnerabilities on exposed systems.** CISA's Known Exploited Vulnerabilities catalog lists flaws confirmed as attacked in the wild, 1,766 entries at the time of writing, and CISA recommends using it as an input to patching priority [11]. Restricting the count to internet-facing systems keeps the number small enough to reach zero.

**Critical vendor concentration.** This row counts dependencies, independent of spend. It includes the cloud region that runs every customer system, the payroll processor, and any service desk that can reset a password, as in the Clorox case [10].

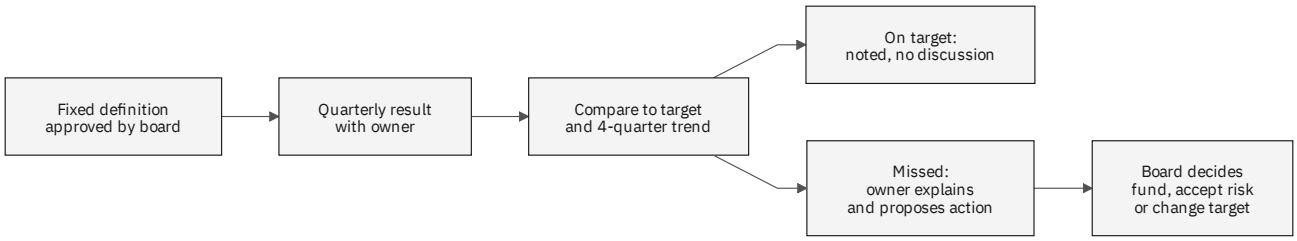
**Change failure rate.** Google's DORA research program, the long-running DevOps Research and Assessment study, defines change fail rate as the share of deployments that need immediate intervention afterward [12]. In the author's experience it is the most useful single indicator of whether engineering changes are under control. The program warns against turning delivery metrics into mandated goals, because teams game them [12], so the board sees the trend and a review threshold rather than a quota.

**Recovery targets met.** Recovery time and data-loss targets are business decisions the board should have approved. This row reports whether they held, in tests and in real events.

**AI systems in production.** The NIST AI Risk Management Framework, released in January 2023 [13], expects mechanisms to inventory AI systems, resourced according to risk (GOVERN 1.6) [14]. The board needs the count, the owner of each system, and when each was last evaluated.

---

**Exhibit 2. How the report turns a measure into a board decision**




Source: author's framework.

The flow above is the point of the format. Measures on target take no meeting time. Measures that missed get the discussion, and the discussion ends in a recorded choice: fund a fix, accept the risk with a date to revisit, or change the target. That record is what a 10-K description of board oversight should rest on [1].

SIDEBAR: WHY SIX, AND WHY THESE

Each row answers a question a director will be asked after an incident: could we recover, were we exposed to a known attack, did one supplier take us down, did our own change cause it, did we meet the recovery promise, and who owned the AI that acted. Maturity scores, training completion and phishing click rates are useful to management. They belong in the committee pack, below the six lines.

## Costs, Risks, and Tradeoffs

The report is cheap to produce once the data exists, and expensive when it does not. For many companies the first quarter shows blanks, such as tier-one systems never restore-tested or AI tools with no owner. Those blanks are findings.

**Exhibit 3. Tradeoffs of a fixed quarterly report**

| Area | Cost or risk | Mitigation |
|---|---|---|
| First-year effort | Building the inventories behind each row: tier-one systems, exposed assets, critical vendors, AI systems | Start with tier-one services only; report blanks as "not measured" in red |
| Gaming | Owners narrow definitions to hit targets, such as fewer systems called tier one | Definitions change only with board approval; internal audit samples one row each quarter |
| False comfort | Six green rows can hide a risk outside the report | Keep a short "new risks" section; review the six measures each year |
| Delivery metrics as quotas | Pressure on change failure rate can slow delivery or hide failures [12] | Show trend and review threshold; never tie it to compensation |
| Disclosure exposure | A written record of misses can be read by regulators and plaintiffs | Record the decision taken on each miss; consistency with public statements is the protection [8] |
| When this is wrong | A company with almost no internal systems, running on a few SaaS products, has little to restore or patch | Keep the vendor concentration and AI rows; replace the rest with vendor attestation status and access reviews |

Source: author's analysis.

The disclosure row deserves a direct answer. Some counsel prefer that boards receive less in writing. The October 2024 settlements were about statements that did not match what the companies knew [8]. A board that receives the facts consistently is in a better position to keep public statements accurate.

# How to Act

**Exhibit 4. A one-year roadmap**

| Window | Actions | Owner | Milestone |
|---|---|---|---|
| First 30 days | Agree on the six definitions and the tier-one service list. Name an owner for each row. Pull whatever data exists today. | CEO with CIO and CISO | Definitions approved by the board or its risk committee; first report drafted, blanks marked |
| First 90 days | Build the inventories: exposed assets, critical vendors with access rights, AI systems with owners. Start quarterly restore tests of tier-one systems. | CIO, CISO, COO | First full report with all six rows populated; at least 25% of tier-one systems restore-tested |
| First 90 days | Propose targets for each row with cost of meeting them. | Each row owner | Board approves targets and records any risk it accepts |
| First 365 days | Report every quarter in the same format with history. Internal audit tests one row per quarter. Align the 10-K description of board oversight with the report. | CFO with general counsel and internal audit | Four consecutive quarters reported; every tier-one system restore-tested within the year; zero exploited flaws on exposed systems past deadline; every AI system with an owner |

Source: author's recommendation.

# Questions to Ask Your Team

1. Which of our systems are tier one, and when was each last restored from backup in a test?
2. How many flaws on CISA's exploited list are open on our internet-facing systems today, and how old is the oldest?
3. Which vendors could stop a critical business function on their own, and which can reset our employees' credentials?
4. What share of our production changes needed a rollback or emergency fix last quarter, and is that rising?
5. Did we meet our approved recovery times in every test and incident this year?
6. How many AI systems and agents do we run in production, and who owns each one?
7. Does what we wrote in our last 10-K about board oversight match what the board actually receives?

## Closing

Directors are accountable for technology risk in disclosure and, for EU financial firms, in regulation. They cannot oversee what changes form every meeting. Approve six measures, give each an owner and a target, and receive them every quarter with a year of history. Spend the meeting on the rows that missed, and record what the board decided.

# Sources

[1] U.S. Securities and Exchange Commission. "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies." Press Release 2023-139. 2023. https://www.sec.gov/newsroom/press-releases/2023-139.

[2] EY Center for Board Matters. "Cyber and AI oversight disclosures: what companies shared in 2025." 2025. https://www.ey.com/content/dam/ey-unified-site/ey-com/pt-br/campaigns/board-matters/documents/ey-cbm-cyber-and-ai-oversight-disclosures-2025-3.pdf.

[3] Gartner. "Gartner Survey Finds 90 Percent of Non-Executive Directors Lack a Measure of Confidence in Cybersecurity Value." Press release, 2026 Gartner Board of Directors Survey. 2025. https://www.gartner.com/en/newsroom/press-releases/2025-11-24-gartner-survey-finds-90-percent-of-non-executive-directors-lack-a-measure-of-confidence-in-cybersecurity-value. Detailed figures as reported by FinTech BizNews, "90% NEDs Lack Trust In Cybersecurity Value." 2025. https://fintechbiznews.com/fintech-it-security/90-neds-lack-confidence-in-cybersecurity-value.

[4] National Association of Corporate Directors. "Director's Handbook on Cyber-Risk Oversight: Principles." 2026 edition. 2026. https://prod.nacdonline.org/all-governance/governance-resources/governance-research/director-handbooks/2026-cyber-risk-oversight/cyber-risk-handbook-principles-2026/.

[5] National Institute of Standards and Technology. "The NIST Cybersecurity Framework (CSF) 2.0." NIST CSWP 29. 2024. https://doi.org/10.6028/NIST.CSWP.29.

[6] EUR-Lex. "Digital operational resilience for the financial sector." Summary of Regulation (EU) 2022/2554. https://eur-lex.europa.eu/EN/legal-content/summary/digital-operational-resilience-for-the-financial-sector.html.

[7] Regulation (EU) 2022/2554 (Digital Operational Resilience Act), Article 5, "Governance and organisation." OJ L 333, 27.12.2022. 2022. Text as reproduced by Springlex. https://www.springlex.eu/en/packages/dora/dora-regulation/article-5/.

[8] U.S. Securities and Exchange Commission. "SEC Charges Four Companies With Misleading Cyber Disclosures." Press Release 2024-174. 2024. https://www.sec.gov/newsroom/press-releases/2024-174.

[9] Harvard Law School Forum on Corporate Governance. "SolarWinds Dismissed: What the SEC's U-turn Signals for Cyber Enforcement." 2025. https://corpgov.law.harvard.edu/2025/12/07/solarwinds-dismissed-what-the-secs-u-turn-signals-for-cyber-enforcement/.

[10] The Register. "$380M lawsuit claims intruder got Clorox's passwords from Cognizant simply by asking." 2025. https://www.theregister.com/2025/07/23/lawsuit_clorox_vs_cognizant/.

[11] Cybersecurity and Infrastructure Security Agency. "Known Exploited Vulnerabilities Catalog." https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

[12] DORA (DevOps Research and Assessment). "DORA's software delivery performance metrics." https://dora.dev/guides/dora-metrics/.

[13] National Institute of Standards and Technology. "AI Risk Management Framework." NIST AI 100-1. 2023. https://www.nist.gov/itl/ai-risk-management-framework.

[14] National Institute of Standards and Technology. "AI RMF 1.0, GOVERN 1.6: Mechanisms are in place to inventory AI systems." Subcategory text as catalogued by STIG Viewer. https://www.stigviewer.com/controls/ai-rmf/GOVERN%201.6.

---

The views in this paper are the author's own and do not represent any employer. Scenarios are hypothetical. This paper is not legal, financial, or compliance advice.