THE ANTI-CHECKBOX SECURITY SCORECARD

A 10-minute diagnostic for CFOs, CEOs, and CTOs at product-focused companies

---

Checkbox security produces documents. Anti-checkbox security produces **evidence**—in the SDLC, in production, and in board reporting.

What this scorecard tells you

Whether your security program is reducing real risk—or just generating audit comfort.

Score each item:

1 = "We can show this today."

0 = "We can't."

A) BUILD — Can engineers ship safely without heroics?

☐ **1) Release gates exist (and they're sane).**

Can a developer merge code with critical issues without tripping an automated gate?

`Evidence:` *CI policy that blocks on agreed criticals (secrets, known-exploitable deps, high-risk patterns).*

☐ **2) "Top risks" are designed out early.**

Are threat models attached to your highest-risk epics/features?

`Evidence:` *Last 3 high-risk epics include threat model + security acceptance criteria.*

☐ **3) Ownership is explicit.**

Do your internet-facing services/APIs have named owners?

`Evidence:` *Service inventory with owner + on-call + data sensitivity.*

B) DEPLOY — Is cloud posture controlled by default?

☐ 4) Infrastructure is repeatable, not "snowflake."

Do you deploy via IaC with drift detection?

`Evidence:` *IaC repo + drift alerts or change logs.*

☐ 5) Secrets are managed, not "found."

Are secrets centralized and rotated?

`Evidence:` *Secret manager usage + rotation policy + last rotation proof.*

☐ 6) Access is constrained.

Is privileged access protected (MFA, least privilege, time-bounded elevation)?

`Evidence:` *IAM controls + last access review / approval logs.*

C) RUN — Can you detect, contain, and learn fast?

☐ 7) You can answer: "What data could we lose?"

`Evidence:` *Data map (systems + flows) + tiered classification.*

☐ 8) You can answer: "How fast would we know?"

Do you track MTTD/MTTR for security incidents (even small ones)?

`Evidence:` *Incident log + trends, not anecdotes.*

☐ 9) Post-incident changes actually stick.

`Evidence:` *Last 2 postmortems show a control/process change that is now verifiably in place.*

D) GOVERN — Is the board getting signal, not anxiety?

☐ 10) You have 3 metrics that correlate with risk reduction.

Not "training completed." Not "tickets closed."

`Evidence:` *3 trend lines tied to exploitability / blast radius / response time. ("Metrics that matter.")*

☐ 11) Exceptions are time-bounded.

`Evidence:` *Risk register with owner + expiry date + compensating control.*

☐ 12) Compliance is produced from evidence.

`Evidence:` *Control mappings point to real system artifacts (configs, logs, pipelines), not slide decks.*

SCORING

0–4 **Security Theater Risk** You may pass audits and still be fragile.

5–8 **Fragile but Fixable** You have pieces—gaps are creating "panic cycles."

9–12 **Operational Security System** Security runs continuously. Exec conversations are evidence-based.

If you scored 0–8: the fastest path to "anti-checkbox"

Do these 3 things in the next 30 days:

1. Install sane build/release gates that don't slow product teams.
2. Create an owned inventory (services + owners + data sensitivity).
3. Pick 3 board metrics and report them monthly—no stories, just trends.

Want help implementing this?

Contact Asgard Security for a 30-minute diagnostic call.

security@asgardsec.com | www.asgardsec.com

Security that protects. Not security that pretends.