AI SECURITY READINESS CHECKLIST

Is Your AI Deployment Ready for Board Scrutiny?

Use this checklist to quickly assess whether your current AI systems, workflows, and governance are prepared for executive and regulatory review. Each section reflects the exact topics boards, auditors, and regulators are already asking about in 2025.

---

1. Model Risk & Alignment

□ Have you documented the model's capabilities, limitations, and high-risk failure modes?
□ Do you track jailbreak susceptibility with ongoing adversarial testing?
□ Have you evaluated autonomy, instruction-following deviation, and goal-drift risks?
□ Is every model version (internal or vendor) mapped to a risk profile?

---

2. Data Protection & Supply Chain Integrity

□ Is all training, fine-tuning, and inference data governed with clear access controls?
□ Do you validate datasets for poisoning, contamination, bias, and leakage?
□ Are third-party APIs, open-source models, and embeddings tracked for security risk?
□ Do you have SBOM-equivalent visibility for all AI components?

---

3. Adversarial Resilience

□ Has your system undergone independent AI red teaming in the last 6–12 months?
□ Do you have continuous red teaming or automated adversarial discovery?
□ Is your model resistant to prompt injection, escalation, impersonation, and extraction?
□ Can you detect malicious user patterns (automated probing, multi-turn bypassing)?

---

4. Governance, Policies & Human Oversight

□ Do you maintain a documented AI governance structure with defined owners?
□ Is there a clear, enforced employee AI use policy?
□ Are deployment, rollback, and safety-signoff decisions logged and reviewable?
□ Is there required human oversight for high-risk use cases?

---

5. Monitoring, Logging & Incident Response

□ Do you have real-time monitoring for model drift, hallucination spikes, and misuse?
□ Is AI-specific anomaly detection in place (e.g., autonomy drift, content deviation)?
□ Are model logs retained in a secure, reviewable, privacy-compliant manner?
□ Does your IR playbook include AI-specific incident types and escalation paths?

---

6. Compliance & Enterprise Risk

□ Are you aligned with NIST AI RMF, OWASP AIVSS, and CSA MAESTRO guidance?
□ Are high-risk AI systems formally reviewed through your enterprise risk program?
□ Can you produce a board-ready narrative on AI safety, reliability, and ROI?
□ Do you maintain documentation showing continuous improvement?

Scoring Guide

Count each checked box.

0–10 checks: High risk. You're exposed to regulatory, reputational, and operational failures.

11–18 checks: Moderate maturity but with significant blind spots. You need targeted remediation.

19–24 checks: Strong posture with clear governance — ready for board-level review.

Next Step

To receive a detailed assessment of your posture, including prioritized risks and action plans:

Request a confidential consultation

Email david@mrcampbell.org