

TRE AI GOVERNANCE & MANAGED RESILIENCE CHECKLIST

A board-ready baseline for identifying the AI Risk Intelligence Gap

Most organizations are scaling SaaS, cloud, and AI faster than their risk and control models can adapt. Use this checklist to baseline the autonomous enterprise and identify the highest-priority governance gaps.

PHASE 1: ASSESS - Mapping the Risk Intelligence Gap

- [] **Audit the Knowledge Layer (RAG):** Have we determined exactly what internal data our AI systems and public answer engines are retrieving?
- [] **Prevent Automated Risk:** Are AI agents prevented from pulling unstructured, unverified, or sensitive compliance data?
- [] **Execute a T2V Assessment:** Can we measure the velocity of value for cloud and AI investments, or are they expanding the attack surface?
- [] **Define the Minimum Viable Business:** Has leadership identified the systems, AI dependencies, and workflows essential for survival during a major outage?

PHASE 2: INFLUENCE - Engineering the Control Tower

- [] **Govern Non-Human Identity:** Have machine-to-machine identities, AI agents, and automated workflows been secured and assigned accountable owners?
- [] **Anchor to Verified Truth:** Are authoritative knowledge pipelines in place so AI outputs are grounded in verified information?
- [] **Bridge the Silos:** Is there a working agreement between the CMO driving AI visibility and the CISO defending enterprise trust?
- [] **Engineer Trust into Speed:** Can business units deploy approved AI capabilities quickly through pre-vetted architectures and guardrails?

PHASE 3: RESILIENCE - Continuous Output Governance

- [] **Protect AI Brand Trust:** Are we monitoring how major answer engines describe the organization, recommend its services, and cite its data?
- [] **Establish Drift Detection:** Can we identify material changes in data, model behavior, citations, and recommendations before they create harm?
- [] **Automate Guardrails:** Have manual compliance checklists begun moving toward dynamic, repeatable risk-readiness controls?
- [] **Demand Outcome-Driven Metrics:** Does the board receive evidence that business risk has been reduced, not only activity counts?

YOUR NEXT STEP

If you cannot confidently answer yes to these questions, schedule a complimentary 30-minute TRE AI Brand Risk Pulse Session. You will receive a focused posture readout, a vulnerability walkthrough, and one immediate corrective action.

Strategy matters. Execution decides. Let's make speed safe.