

THE T.E.S.T. FRAMEWORK™ CHECKLIST

A Practical Framework & Risk Assessment Tool for Educational & Enterprise Leaders

AI is already inside your organization. Most leaders just don't know where.

You don't have an AI problem—you have a *visibility* problem. The T.E.S.T. Framework™ is a defensible AI risk-scoring engine trusted by CIOs, CISOs, procurement teams, and educational leaders to evaluate AI tools in 60 seconds before deployment. This practical framework bridges the gap between written policy and real-time execution, giving leaders board-ready assurance.

THE FOUR PILLARS OF T.E.S.T.™

T.E.S.T. breaks AI risk management down into four easily understandable dimensions of assessment:

- T TOUCH**
Does it access sensitive data?
Evaluate data exposure risk. Map every student, employee, or customer touchpoint and classify input data sensitivity before integration.

E EXECUTE
Can it take actions or decide?
Analyze execution autonomy. Define human-in-the-loop oversight checkpoints, bias/accuracy checks, and review workflows for AI decisions.
- S STORE**
Is data stored or sent externally?
Track data custody. Vet vendor practices, enforce secure storage, and verify regulatory compliance with FERPA, HIPAA, or state privacy laws.

T TRUST
Can it be audited & defended?
Ensure accountability. Publish an active AI governance policy, appoint owners, and maintain a defensible, auditable chain of decision-making.

60-SECOND AI RISK SCORING ENGINE

For a rapid initial assessment of any individual AI tool, score each of the four pillars from 1 (Low Exposure) to 5 (High Exposure) using the formula: **T + E + S + T = Risk Score (4–20)**.

Risk Classification	Score Range	Decision Protocol & Required Actions
■ LOW RISK	4 – 8	PROCEED. Approve deployment with standard operational monitoring. Low data and action exposure.
■ MODERATE RISK	9 – 14	PROCEED WITH CONTROLS. Deploy only after adding active human oversight and compliance safeguards.
■ HIGH RISK	15 – 20	DO NOT DEPLOY (REJECT). Deny procurement or block deployment. Resolve identified security or ethical gaps, then re-evaluate.

NIST AI RISK MANAGEMENT FRAMEWORK (AI RMF) ALIGNMENT

The federal NIST AI RMF is the gold standard for responsible AI governance. The T.E.S.T. Framework™ operationalizes its core functions into standard workflows: **Touch** executes the **MAP** function; **Execute & Store** quantify risks for **MEASURE**; **Trust** drives **GOVERN**; and the total scoring engine delivers **MANAGE**. T.E.S.T. gives your organization a practical, highly defensible way to demonstrate compliance with federal AI standards in front of regulators, auditors, and boards.

THE FULL T.E.S.T.™ GOVERNANCE AUDIT

Use this comprehensive audit checklist to measure your organization's systemic AI governance posture. Check each statement that is fully true for your institution.

✓	Evaluation Criterion	NIST AI RMF
T — TOUCH: DATA ACCESS & INVENTORY CONTROL		
☐	All AI tools in use across the entire organization are fully inventoried	MAP
☐	Shadow AI usage (unauthorized software) has been actively identified and documented	MAP
☐	Employees and departments know exactly which AI tools are approved vs. unapproved	MAP
☐	AI touchpoints with customers, clients, or student learning workflows are mapped	MAP
☐	All organizational departments have fully disclosed any AI tools embedded in workflows	MAP
E — EXECUTE: ACTION AUTONOMY & OVERSIGHT		
☐	AI use cases are formally documented with a verified and clear business purpose	MEASURE
☐	SOPs exist detailing how generative AI outputs are reviewed before any execution is finalized	MEASURE
☐	AI-driven actions and decisions have mandatory human-in-the-loop oversight checkpoints	MEASURE
☐	Deployments and workflows include continuous checks for output bias, drift, and accuracy	MEASURE
☐	Clear roles, responsibilities, and permissions for AI-assisted execution are established	MEASURE
S — STORE: DATA STORAGE, CUSTODY & COMPLIANCE		
☐	Data inputs fed into AI systems are rigorously classified by privacy and security sensitivity	MEASURE
☐	AI data storage practices comply with regulatory requirements (FERPA, HIPAA, GDPR, etc.)	MEASURE
☐	Strict access controls are enforced for both AI model training sets and output repositories	MEASURE
☐	Data retention, archival, and deletion policies explicitly cover AI-generated content	MEASURE
☐	Third-party AI vendors' data processing, logging, and security compliance has been fully assessed	MEASURE
T — TRUST: ETHICS, AUDITABILITY & ACCOUNTABILITY		
☐	An official AI governance policy is formally published, updated, and communicated	GOVERN
☐	AI-specific exposure is actively registered and tracked in the enterprise risk register	GOVERN
☐	Organizational leadership and staff have completed mandatory AI literacy and governance training	GOVERN
☐	Third-party AI tools are continuously vetted against ethical, security, and compliance standards	GOVERN
☐	A designated AI governance owner, security leader, or oversight committee is actively in place	GOVERN

SYSTEMIC RISK EVALUATION SCORING GUIDE

Count your checked criteria to determine your organization's final AI Governance Posture:

■ 0 – 8 Checked: **High Risk / High Exposure** (Immediate remediation required) | ■ 9 – 14 Checked: **Moderate Risk** (Implement safeguards) | ■ 15 – 20 Checked: **Strong Posture** (Maintain oversight)

READY TO SYSTEMATIZE YOUR AI GOVERNANCE?

■ BOOK A T.E.S.T. REVIEW SESSION

One-on-one executive guidance to score your AI tool catalog, identify critical exposure vectors, and prepare board-ready reporting pipelines.

■ BRING T.E.S.T. TO YOUR INSTITUTION

Deploy the full framework across your organization with customized compliance scorecards, training programs, and operational support.

Secure your organization's digital transformation with a defensible AI strategy today.

Contact **Teri D. Green**, Vice President of Technology, directly at greent@theethicsengine.com or visit lite-technology-solutions.sintra.site to schedule your review session.