Tennessee Audit Teams Using AI

Southwest/Southeastern Intergovernmental Audit Forums (SWIAF/SEIAF) 2026 Summer Webinar

Presented by

Chase Tramel, CISA, CRISC – Legislative IS Audit Manager
Division of State Audit

Tennessee Comptroller of the Treasury

Tennessee Comptroller of the Treasury

The opinions expressed during this presentation are my own. They do not necessarily represent the views of the Tennessee Comptroller of the Treasury, his representatives, or the Tennessee Department of State Audit.

Generative AI Tools

Microsoft CoPilot Chat

Web-Only Platform

Best for General Questions and Research

Available to Everyone

Microsoft 365 CoPilot

Web & Integrated Platform

Best for Daily Workflows & In-app Generation

Must be Requested**

OpenAI ChatGPT Enterprise

Standalone Platform and Features

Best for Specialized Tasks

Must be Requested**

** - Licenses are held to a "Use it or Lose it" policy every billing cycle.

TENNESSEE COMPTROLLER OF THE TREASURY

Office Due Diligence for Generative AI

Reviewed Tools with Security in Mind

- Evaluated Microsoft 365 CoPilot, CoPilot Chat, and ChatGPT for potential use.
- Considered confidentiality laws (TCA 10-7-504(i), FERPA, PHI, CJIS, FTI)

Lessons from Pilot Group

- Tools help with brainstorming, writing clarity, and plain-language communication.
- Require human judgment—outputs must always be verified

Safeguards in Place

- Use only approved and authorized accounts.
- Never upload sensitive or restricted data.
- Treat AI as an assistant, **not a decision maker**.

TENNESSEE COMPTROLLER OF THE TREASURY

Key Challenges of AI Adoption

Governance

"Can we use AI safely and responsibly?"

Capability

"Do our people know how to use AI effectively?"

Operational Integrity

"Can we use AI consistently and sustainably?"

TENNESSEE COMPTROLLER OF THE TREASURY

Core AI Use Cases

RESEARCH

PLANNING

ANALYSIS

REPORTING

COMMUNICATION

TOOL DEVELOPMENT

TENNESSEE COMPTROLLER OF THE TREASURY

Core AI Use Cases

RESEARCH PLANNING

Third-Party Risk RACI

I have a third-party risk situation within the government sector, and I would like you to assume the roles of an experienced third-party risk practitioner, an experienced internal auditor, and a chief risk officer. I would like to create a RACI table at the enterprise level for the parties involved—Agency1 (Owner/Accountable), Agency2 (Secondary Party/Responsible), and Vendor1 (Third Party/Responsible). Agency2 may serve as a subject matter expert who may need to be informed so that they may consult. Provide the best practices and/or third-party framework that you use for developing my request.

For your scenario, I would approach this from three complementary perspectives:

- **Third-Party Risk Practitioner** – focused on lifecycle governance, vendor accountability, and risk ownership.
- **Internal Auditor** – focused on segregation of duties, evidence, controls, and auditability.
- **Chief Risk Officer (CRO)** – focused on enterprise governance, accountability, regulatory compliance, and risk oversight.

This is a common operating model in government organizations where one agency owns the mission, another provides shared services or subject matter expertise, and a third-party vendor performs contracted services.

Best Practice Frameworks

Rather than relying on a single framework, I recommend using a hybrid model because each framework addresses a different aspect of third-party risk.

Framework	Purpose	Application to Your RACI
NIST SP 800-161 Rev.1	Cyber Supply Chain Risk Management	Defines supplier governance responsibility
NIST SP 800-53 Rev.5	Security & Privacy Controls	Control ownership and assess responsibilities

Enterprise Accountability Model

I recommend the following ownership philosophy.

Agency1

Business Owner

- Owns the mission
- Owns the contract
- Owns the risk
- Accepts residual risk
- Accountable for regulatory compliance

This should be the **single Accountable (A)** organization.

Agency2

Supporting Government Organization

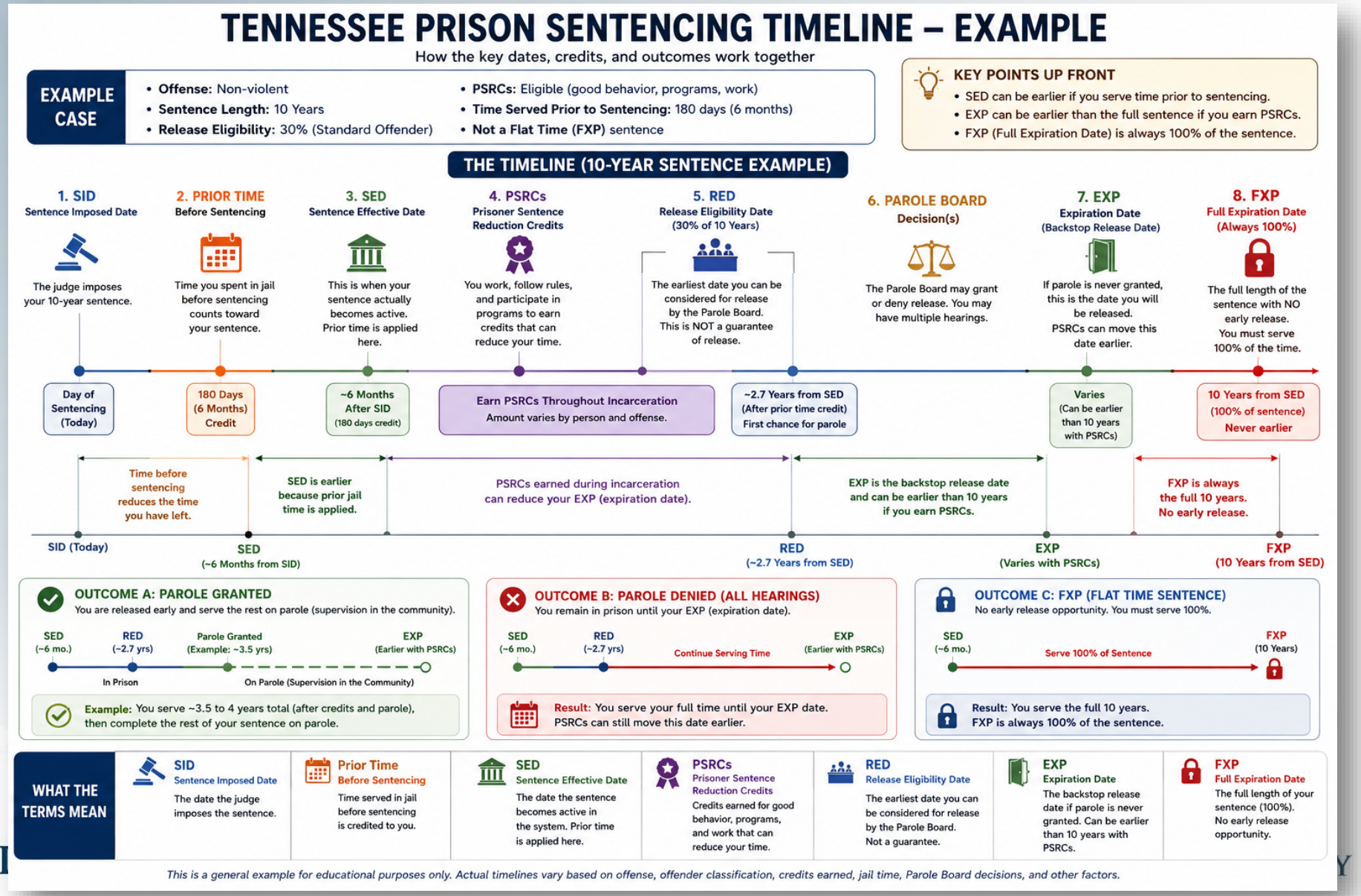
Enterprise Third-Party RACI

Activity	Agency1	Agency2	Vendor1
Business Need Identification	A	C	I
Vendor Selection	A	C	I
Procurement Support	A	C	I
Contract Requirements	A	C	C
Security Requirements Definition	A	R	C
Risk Assessment	A	R	C
Due Diligence	A	R	R
Architecture Review	A	R	C
Privacy Review	A	R	C

Core AI Use Cases

REPORTING

Complex Process Mapping Concept

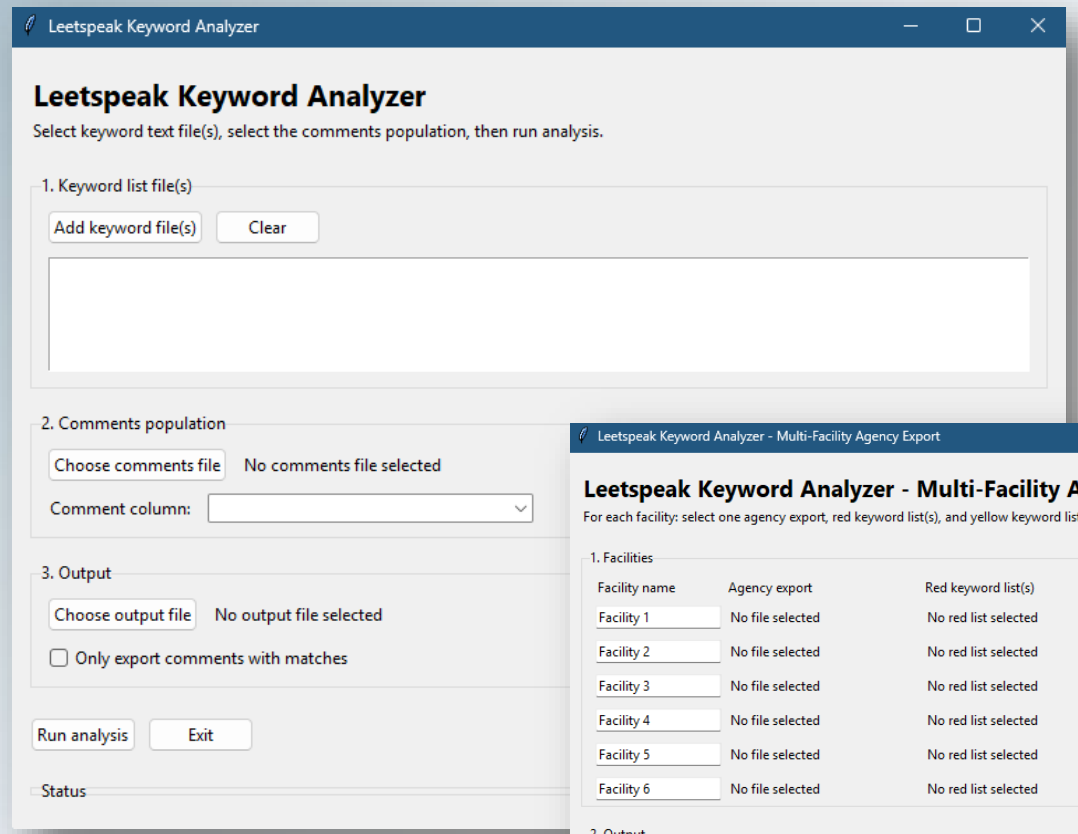


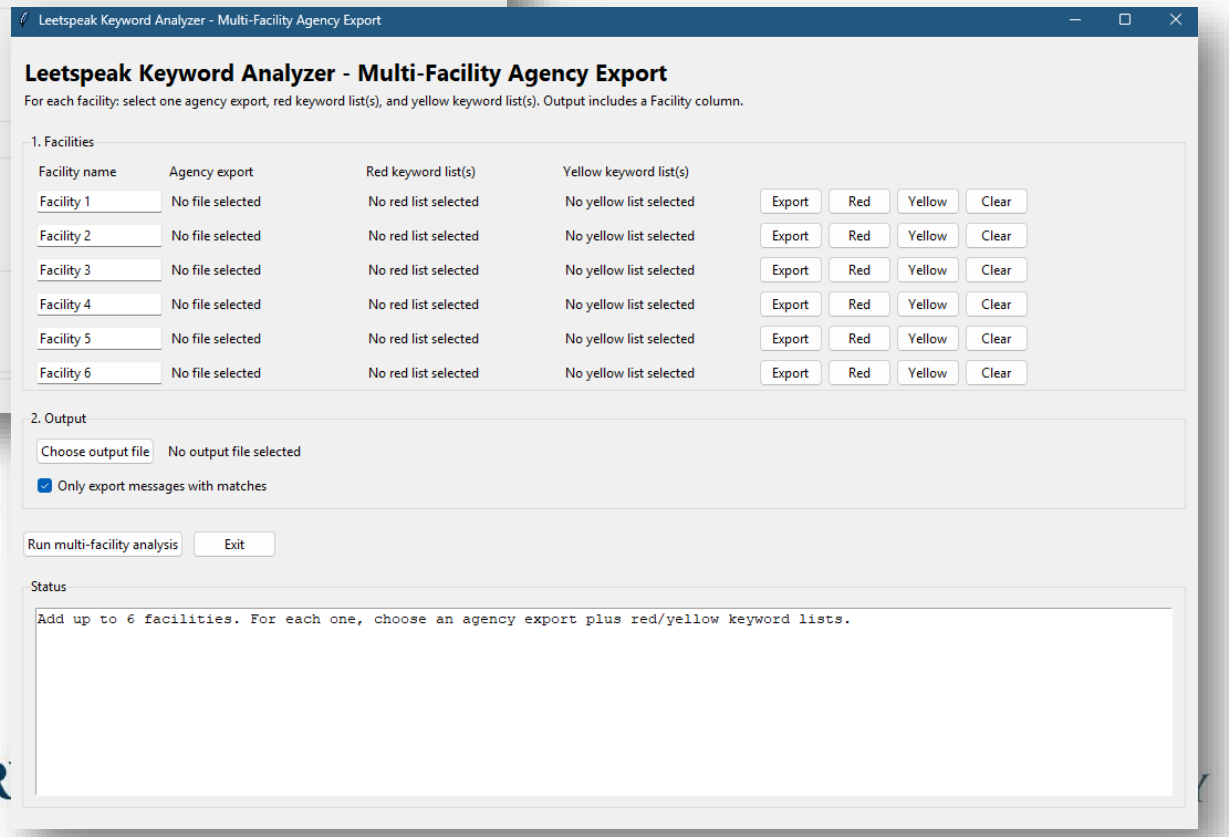
TENNESSEE COMPTROL

Core AI Use Cases

TOOL DEVELOPMENT

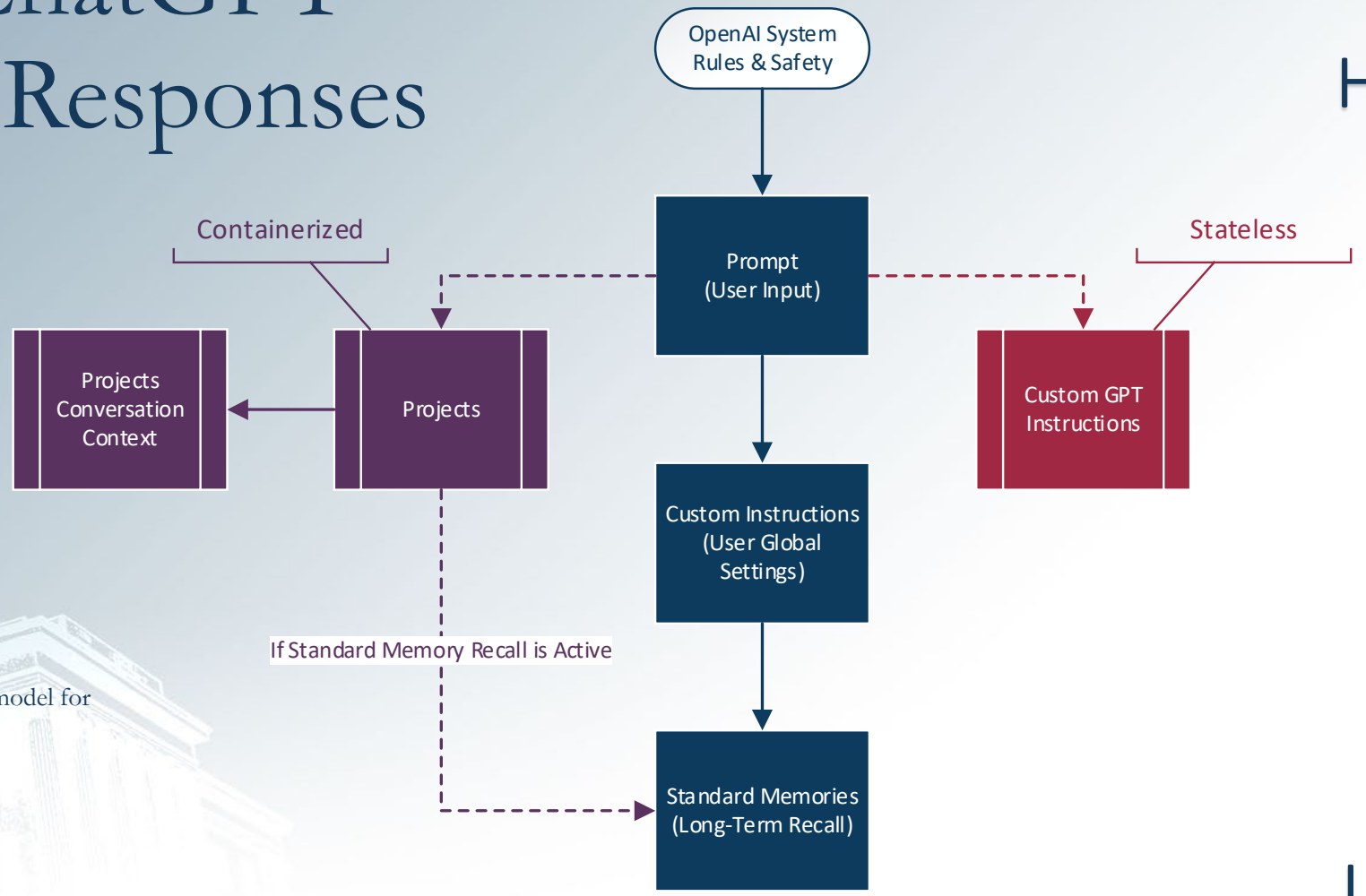
Python-based Leetspeak Keyword Analyzer





TENNESSEE COMPTROLLER OF THE TREASUR

How ChatGPT Builds Responses



Simplified conceptual model for educational purposes

TENNESSEE COMPTROLLER OF THE TREASURY

Prompt Control Signals

Most high-quality prompts combine one signal from each category rather than stacking many similar ones. For example:

"Conduct a forensic, first-principles review of this proposal. Identify material assumptions, red-team the reasoning, and propose orthogonal alternatives."

Control Signal	Typical Effect	Example
Forensic	Deep investigation, evidence-focused analysis	"Perform a **forensic** review of this proposal."
First-Principles	Breaks assumptions down to fundamentals	"Analyze this problem from **first-principles**."
Material	Focuses only on consequential factors	"Identify **material** risks."
Red-Team	Generates critiques and failure modes	"**Red-team** this business strategy."
Orthogonal	Generates alternative perspectives	"Suggest **orthogonal** solutions."

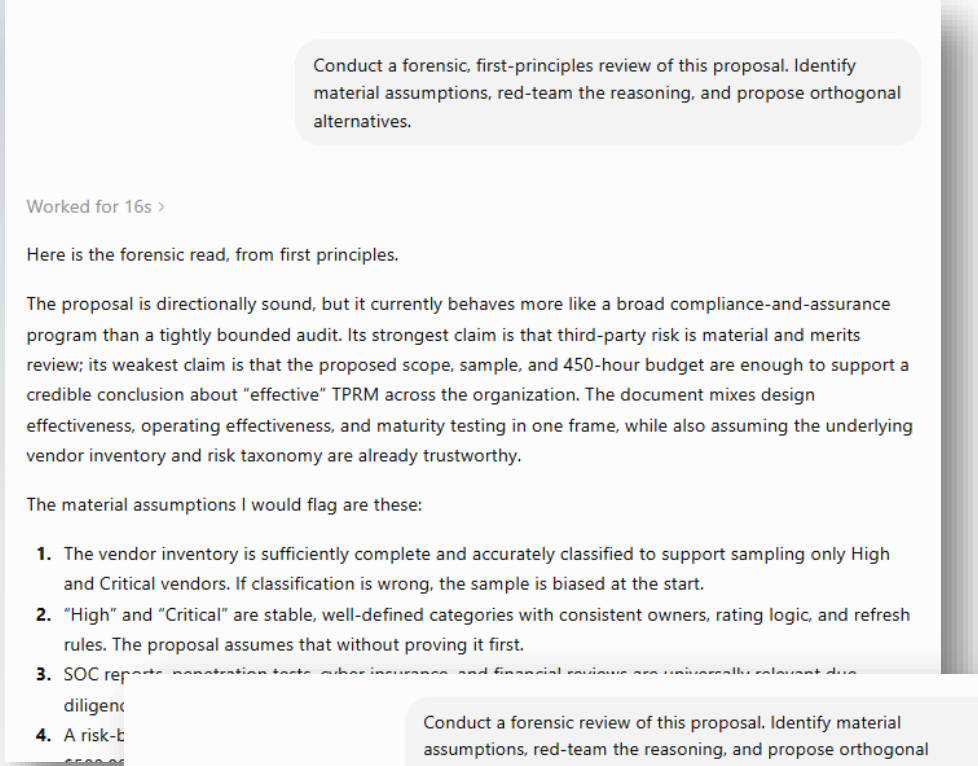
TENNESS

TENNESSEE COMPTROLLER OF THE TREASURY

Prompt Control Signals

A useful mental model is that the strongest control signals tend to activate one of five modes:

1. **Investigate** → forensic, diagnostic, root-cause
2. **Challenge** → red-team, adversarial, skeptical
3. **Model** → mechanistic, causal, first-principles
4. **Prioritize** → material, decisive, high-leverage
5. **Explore** → orthogonal, counterfactual, divergent



Conduct a forensic, first-principles review of this proposal. Identify material assumptions, red-team the reasoning, and propose orthogonal alternatives.

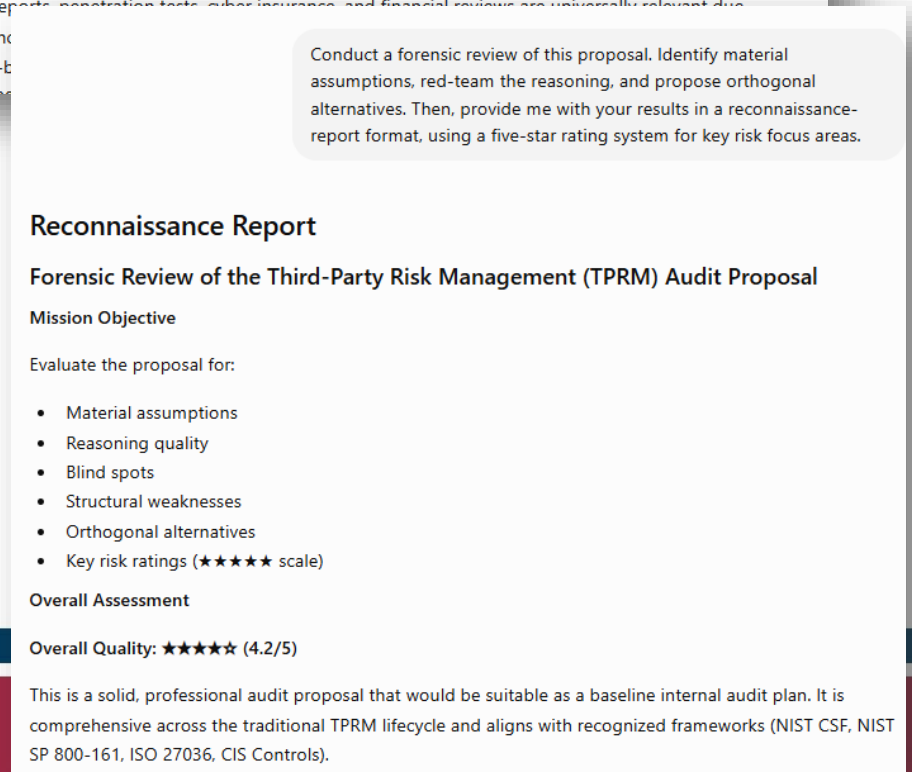
Worked for 16s ›

Here is the forensic read, from first principles.

The proposal is directionally sound, but it currently behaves more like a broad compliance-and-assurance program than a tightly bounded audit. Its strongest claim is that third-party risk is material and merits review; its weakest claim is that the proposed scope, sample, and 450-hour budget are enough to support a credible conclusion about "effective" TPRM across the organization. The document mixes design effectiveness, operating effectiveness, and maturity testing in one frame, while also assuming the underlying vendor inventory and risk taxonomy are already trustworthy.

The material assumptions I would flag are these:

1. The vendor inventory is sufficiently complete and accurately classified to support sampling only High and Critical vendors. If classification is wrong, the sample is biased at the start.
2. "High" and "Critical" are stable, well-defined categories with consistent owners, rating logic, and refresh rules. The proposal assumes that without proving it first.
3. SOC re
diligenc
4. A risk-b



Conduct a forensic review of this proposal. Identify material assumptions, red-team the reasoning, and propose orthogonal alternatives. Then, provide me with your results in a reconnaissance-report format, using a five-star rating system for key risk focus areas.

Reconnaissance Report

Forensic Review of the Third-Party Risk Management (TPRM) Audit Proposal

Mission Objective

Evaluate the proposal for:

- Material assumptions
- Reasoning quality
- Blind spots
- Structural weaknesses
- Orthogonal alternatives
- Key risk ratings (★★★★★ scale)

Overall Assessment

Overall Quality: ★★★★☆ (4.2/5)

This is a solid, professional audit proposal that would be suitable as a baseline internal audit plan. It is comprehensive across the traditional TPRM lifecycle and aligns with recognized frameworks (NIST CSF, NIST SP 800-161, ISO 27036, CIS Controls).

Questions or Comments

Chase Tramel, CISA, CRISC

Chase.Tramel@cot.tn.gov

Office: 615-401-7939

https://www.linkedin.com/in/chase-tramel-cisa-crisc-99863053/