

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



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

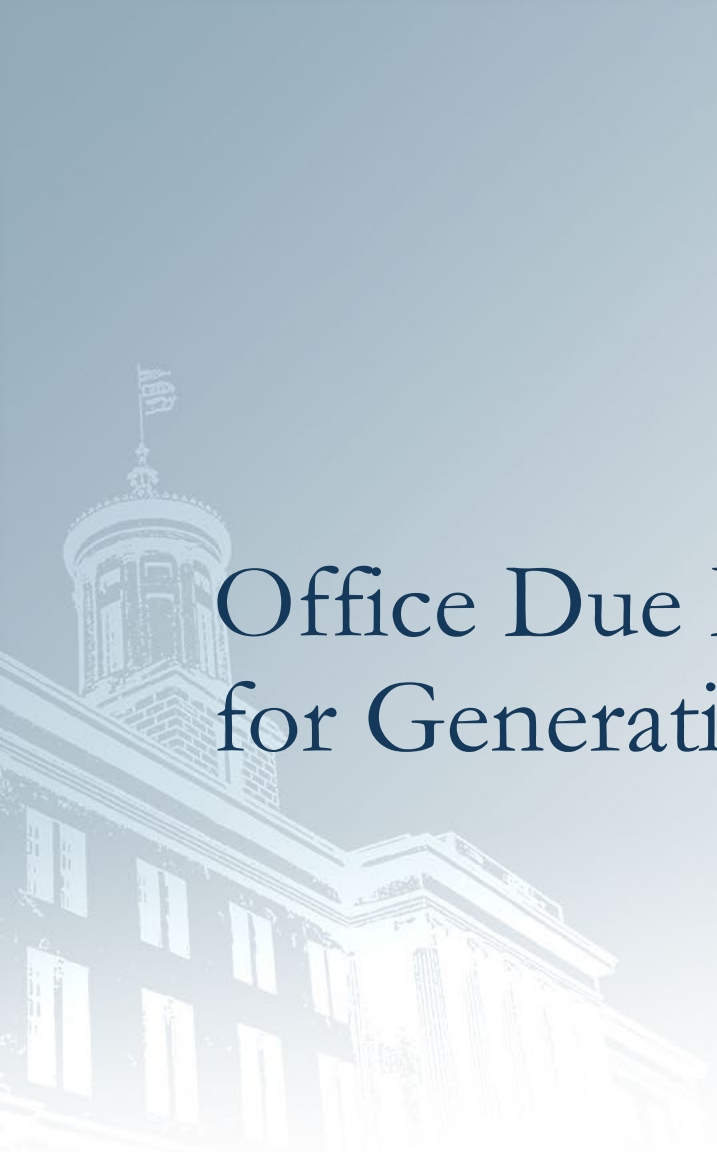
Best for Specialized Tasks

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

TENNESSEE COMPTROLLER OF THE TREASURY

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**.



Key Challenges of AI Adoption



Governance

"Can we use AI safely and responsibly?"



Capability

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



Operational

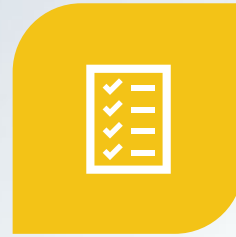
Integrity

"Can we use AI consistently and sustainably?"

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

TENNESSEE COMPTROLLER OF THE TREASURY

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 COMPTROLLER

TENNESSEE PRISON SENTENCING TIMELINE – EXAMPLE

How the key dates, credits, and outcomes work together

EXAMPLE CASE

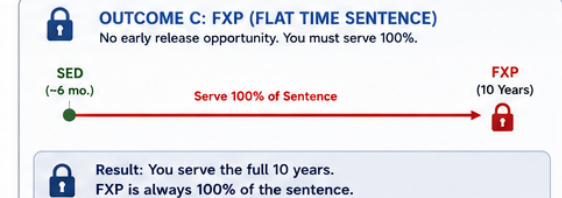
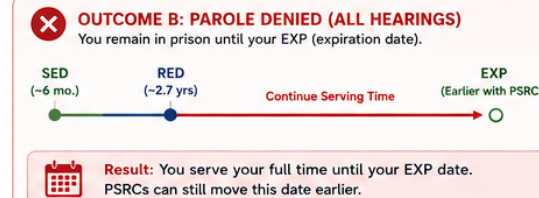
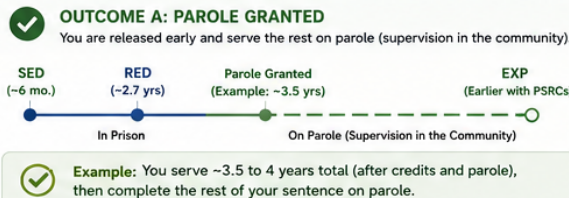
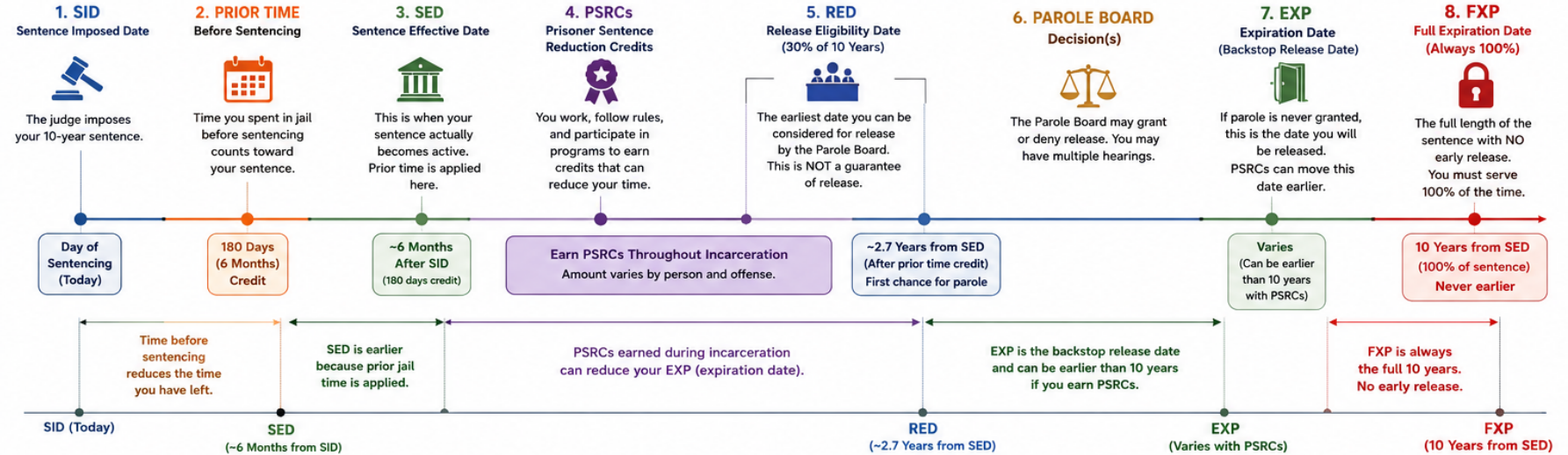
- **Offense:** Non-violent
- **Sentence Length:** 10 Years
- **Release Eligibility:** 30% (Standard Offender)
- **PSRCs:** Eligible (good behavior, programs, work)
- **Time Served Prior to Sentencing:** 180 days (6 months)
- **Not a Flat Time (FXP)** sentence



KEY POINTS UP FRONT

- SED can be earlier if you serve time prior to sentencing.
- EXP can be earlier than the full sentence if you earn PSRCs.
- FXP (Full Expiration Date) is always 100% of the sentence.

THE TIMELINE (10-YEAR SENTENCE EXAMPLE)



WHAT THE TERMS MEAN



SID Sentence Imposed Date
The date the judge imposes the sentence.



Prior Time Before Sentencing
Time served in jail before sentencing is credited to you.



SED Sentence Effective Date
The date the sentence becomes active in the system. Prior time is applied here.



PSRCs Prisoner Sentence Reduction Credits
Credits earned for good behavior, programs, and work that can reduce your time.



RED Release Eligibility Date
The earliest date you can be considered for release by the Parole Board. Not a guarantee.



EXP Expiration Date
The backstop release date if parole is never granted. Can be earlier than 10 years with PSRCs.



FXP Full Expiration Date
The full length of your sentence (100%). No early release opportunity.

This is a general example for educational purposes only. Actual timelines vary based on offense, offender classification, credits earned, jail time, Parole Board decisions, and other factors.

Core AI Use Cases



TOOL
DEVELOPMENT

Python-based
Leetspeak Keyword
Analyzer

TENNESSEE COMPTROLLER OF THE TREASURY

Leetspeak Keyword Analyzer

Select keyword text file(s), select the comments population, then run analysis.

1. Keyword list file(s)

Add keyword file(s) Clear

2. Comments population

Choose comments file No comments file selected

Comment column:

3. Output

Choose output file No output file selected

☐ Only export comments with matches

Run analysis Exit

Status

Leetspeak Keyword Analyzer - Multi-Facility Agency Export

For each facility: select one agency export, red keyword list(s), and yellow keyword list(s). Output includes a Facility column.

1. Facilities

Facility name	Agency export	Red keyword list(s)	Yellow keyword list(s)	Export	Red	Yellow	Clear
Facility 1	No file selected	No red list selected	No yellow list selected	Export	Red	Yellow	Clear
Facility 2	No file selected	No red list selected	No yellow list selected	Export	Red	Yellow	Clear
Facility 3	No file selected	No red list selected	No yellow list selected	Export	Red	Yellow	Clear
Facility 4	No file selected	No red list selected	No yellow list selected	Export	Red	Yellow	Clear
Facility 5	No file selected	No red list selected	No yellow list selected	Export	Red	Yellow	Clear
Facility 6	No file selected	No red list selected	No yellow list selected	Export	Red	Yellow	Clear

2. Output

Choose output file No output file selected

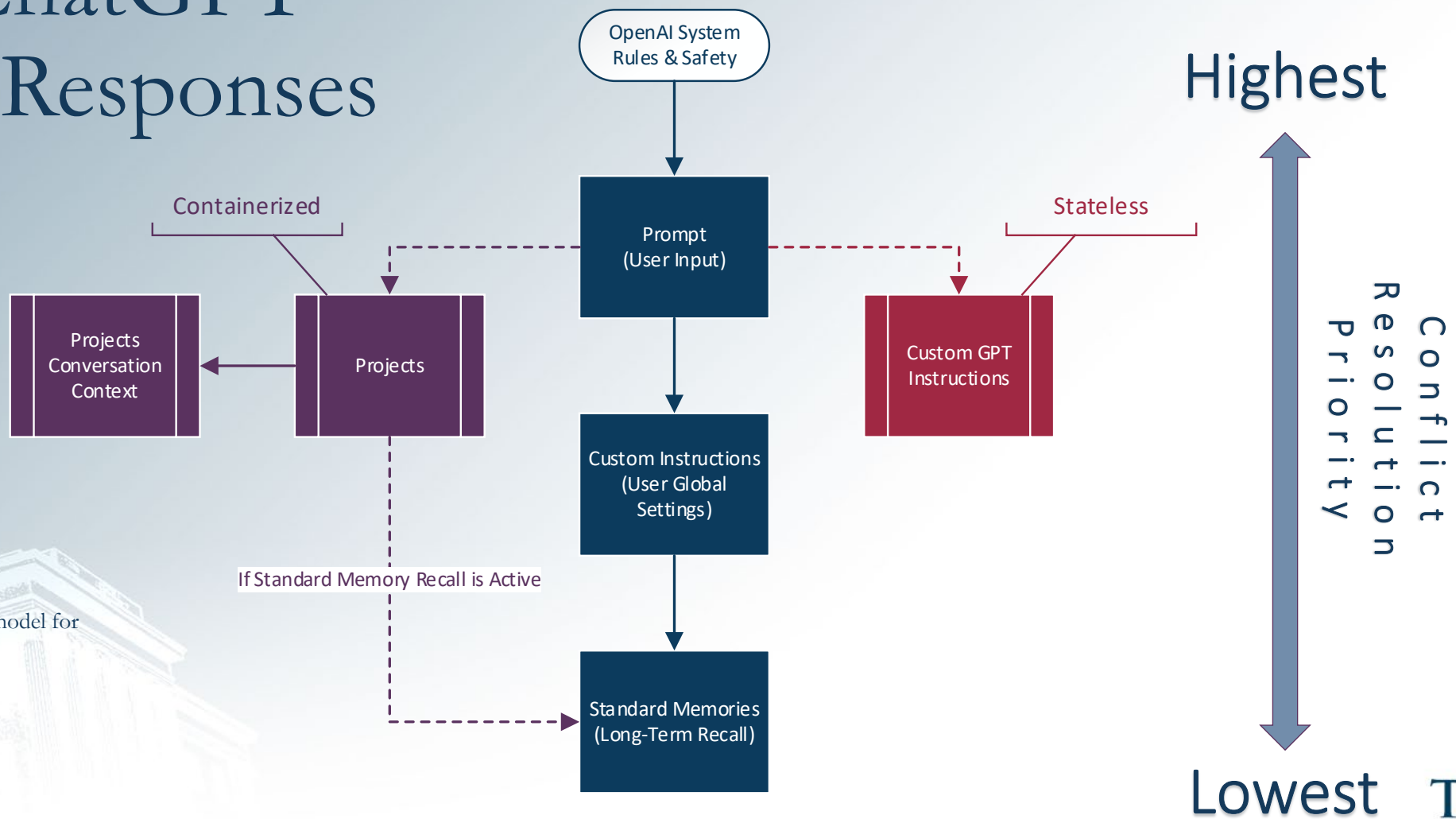
☒ Only export messages with matches

Run multi-facility analysis Exit

Status

Add up to 6 facilities. For each one, choose an agency export plus red/yellow keyword lists.

How ChatGPT Builds Responses



Simplified conceptual model for educational purposes

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 <u>forensic</u> review of this proposal."
First-Principles	Breaks assumptions down to fundamentals	"Analyze this problem from <u>first-principles</u> ."
Material	Focuses only on consequential factors	"Identify <u>material</u> risks."
Red-Team	Generates critiques and failure modes	" <u>Red-team</u> this business strategy."
Orthogonal	Generates alternative perspectives	"Suggest <u>orthogonal</u> solutions."

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

TENNESSEE COMPTROLLER OF THE TREASURY

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 reports, penetration tests, cyber insurance, and financial reviews are universally relevant due diligence.
4. A risk-based approach to sampling is sufficient to ensure representativeness.

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/>

TENNESSEE COMPTROLLER OF THE TREASURY

