TRAIGA FAQ

What Financial Institutions Need to Know

The Texas Responsible AI Governance Act (TRAIGA) is now in effect, and the same core questions keep coming up from the financial institutions we talk to. This FAQ works through them in plain language, so you can get a clear read on your risk, your responsibilities, and your next steps.

1 Is TRAIGA like the EU AI Act? Do we have a big compliance lift ahead?

Short answer: no. TRAIGA is intentionally much narrower and more business-friendly than global frameworks like the EU AI Act.

It does not require:

- Heavy risk classification models
- Broad impact assessments
- Enterprise-wide AI compliance programs

What it does:

- Prohibits specific harmful uses of AI
- Sets expectations for responsible use
- Emphasizes your ability to explain and defend how AI is used

2 If TRAIGA is intent-based, does that mean we're basically fine?

Not quite. TRAIGA uses an intent-based liability standard, meaning the state must show intentional misuse (for example, discrimination).

But your real-world risk comes down to something else: your ability to prove responsible use by knowing where AI is used, understanding what it does, and being able to explain how decisions are made.

3 We already follow GLBA, ECOA, and model risk guidance. Does that cover us?

You're in a strong starting position. TRAIGA does not replace existing regulatory frameworks. It builds on top of them.

4 Is the NIST AI Risk Management Framework required?

Not required but highly recommended. TRAIGA does not mandate a specific framework. However, alignment with recognized frameworks like NIST AI RMF can strengthen your position and provide a defensible, structured approach to AI governance.

5 What's the real risk? Are institutions going to get in trouble?

For most organizations, the immediate risk isn't enforcement. It's exposure.

The biggest gaps we see:

- Not knowing where AI exists (especially in vendor tools)
- No centralized inventory or ownership
- Difficulty explaining how AI impacts decisions

Common warning signs:

- No way to explain or document AI use
- Issues surfacing through complaints, audits, or public scrutiny
- No visible governance structure in place

6 Does TRAIGA require us to disclose all AI use to customers?

Not broadly. TRAIGA does not impose sweeping disclosure requirements across all private-sector use. That said, there is growing expectation, especially in regulated or government-facing contexts, that AI use is transparent. Expectations are evolving alongside examiner and industry trends.

7 What's the role of the regulatory sandbox? Should we care?

TRAIGA includes a 36-month regulatory sandbox that lets organizations test AI systems in a controlled environment and operate with reduced regulatory burden during testing. For most organizations, it's more of an innovation opportunity than a requirement. It's most relevant if you're actively developing or piloting new AI capabilities.

8 What's the first thing we should do?

If you only do three things:

- **Build an AI inventory:** Identify where AI exists, especially across vendors and internal tools
- **Set basic guardrails:** Define acceptable use and human-in-the-loop expectations
- **Establish ownership:** Clarify who is responsible for AI governance and oversight

Where to Start

SBS CyberSecurity can help:

- **AI training:** Enable safe adoption
- **AI risk assessment:** Identify your AI exposure
- **Virtual Chief AI Officer (vCAIO):** Establish governance and oversight

If you'd like help mapping out where your institution stands today, that's the work our team does. We're glad to talk it through whenever the timing's right.

link.sbscyber.com/contact

If you'd rather start on your own, our AI Roadmap lays out the steps in order.

link.sbscyber.com/airoadmap

SBS CyberSecurity

sbscyber.com