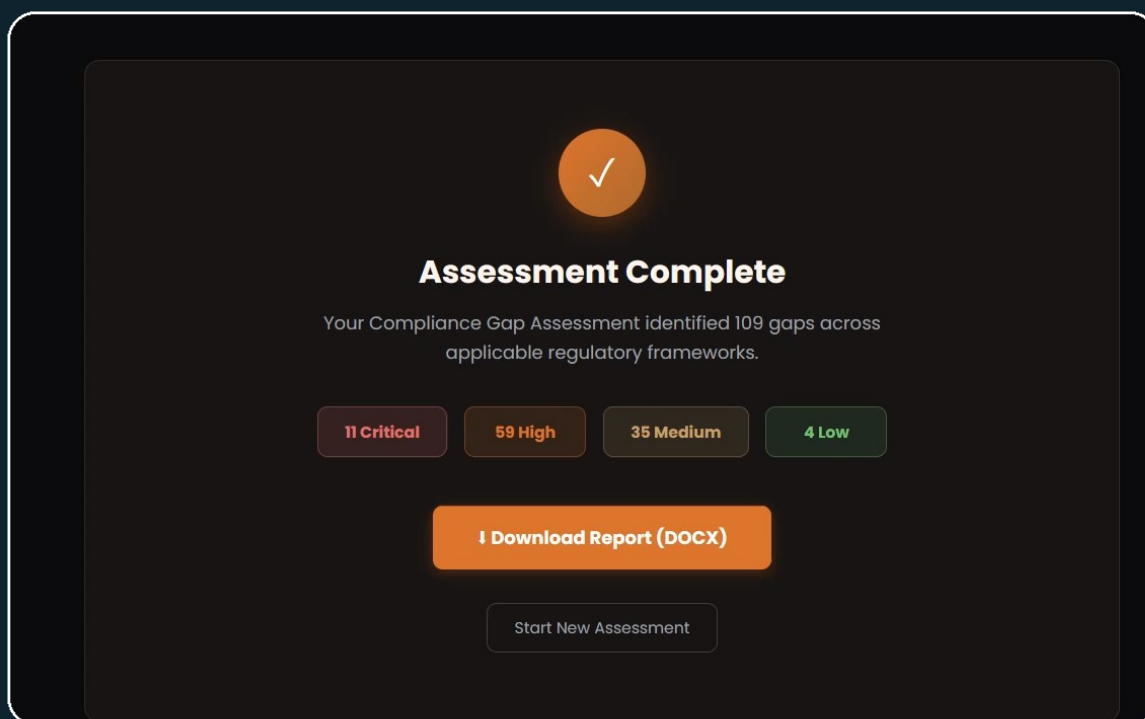


Your Controls May Be Documented.

Can You Prove They Operated?

A practitioner-led walkthrough from one workflow to a defensible starting point



Most governance systems can show that a control exists. The harder question is whether the workflow actually operated as approved.

Authored by Edward J. Beltran, CPA

Former Arthur Andersen and PwC Risk Assurance

THE REQUEST SOUNDS FAMILIAR. THE REAL QUESTION IS DIFFERENT.

A client arrives asking for a framework. The practitioner starts with the organization.

CLIENT PRESSURE

"We need SOC 2."
"We need ISO 27001."
"A customer review is coming."

The request is real. But beginning with the requested framework risks missing the rest of the environment.

PRACTITIONER LENS

What should govern this organization?
What evidence should exist?
What can actually be proven?

The practitioner does not assume the client's requested framework is the complete scope.

1 Describe Your Organization

Be specific. The more detail you provide, the more accurate your gap assessment will be.

SYSTEM NAME *

A short, recognizable name for the system or organization being assessed.

e.g., Customer Risk Analyzer, Clinical Document AI

WHAT DOES YOUR ORGANIZATION DO? *

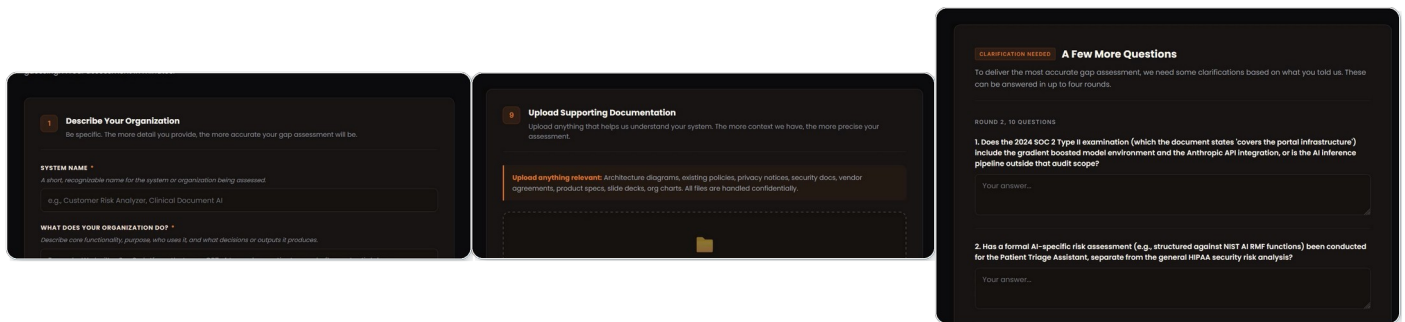
Describe core functionality, purpose, who uses it, and what decisions or outputs it produces.

The journey begins with the company, the system, the data, the geography, and the forcing event - not with a generic checklist.

STEP 1

Start with the organization, not the framework.

The practitioner establishes the facts that drive applicability: what the company does, what data the system touches, where it operates, and what material already exists.



The image shows three sequential screenshots of the Pulse Governance interface. The first screenshot, titled '1 Describe Your Organization', asks for system name and purpose. The second screenshot, titled '2 Upload Supporting Documentation', shows a file upload area. The third screenshot, titled '3 A Few More Questions', shows a series of questions related to the organization's AI usage and risk assessments.

1 · FACTS
2 · DOCUMENTS
3 · CLARIFICATION

- ✓ Uploaded policies, architecture diagrams, and agreements are evaluated for substance - not merely logged as present.
- ✓ Information already established in the intake or documents is not asked again.
- ✓ Follow-up questions are generated from what remains uncertain about this organization.

In traditional GRC, the framework is an input. In Pulse, applicability is an output.

That difference sounds small. It changes everything that follows.

STEP 2

Applicability becomes a reasoned decision - not a checkbox.

The diagnostic evaluates the framework environment in context. Each framework returns one of three states, and the practitioner reviews the rationale before it becomes scope.


APPLIES

Facts establish that the requirement reaches this organization.

DOES NOT APPLY

The exclusion is recorded with the reason that settled it.

NEEDS INPUT

The system asks rather than guessing when the facts do not settle scope.

15 frameworks evaluated

Selected frameworks may guide emphasis. They do not silently limit the analysis.

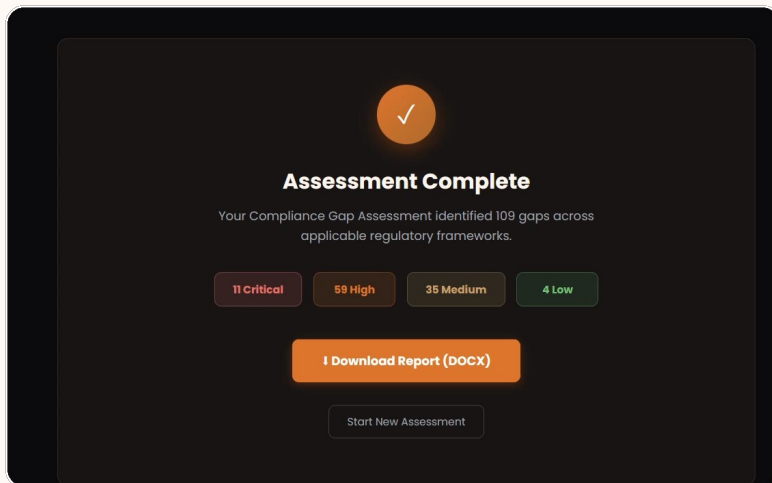
The client stops buying frameworks one at a time. The practitioner sees the full operating environment before remediation begins.

A false inclusion costs review time. A false exclusion can hide an obligation entirely.

STEP 3

The report changes the conversation.

In the synthetic Brazos Diagnostics example, the client did not receive a score and another generic checklist. It received a risk-ranked view of what applies, what exists, what is missing, and what cannot yet be established.



7 applicable frameworks

109 consolidated findings

11 Critical

59 High

35 Medium

4 Low

 AI Governance Gap Assessment <i>Multi-framework assessment produced under the AAIG methodology</i>	
Client	Brazos Diagnostics
AI System	Patient Triage Assistant
Frameworks	ISO 42001 / NIST AI RMF / NIST CSF / SOC 2 / HIPAA / US State AI and Privacy Regulations / Workforce AI Governance
Assessment Date	August 12, 2025
Risk Classification	High (preliminary, the description of clinician review was cut off mid-sentence (Every recommendation is (pg. 3), so the reliability and consistency of the human check before a routing outcome takes effect is not established, and no override or dependency rate is disclosed). The Patient Triage Assistant assigns an urgency score that routes patients into urgent, routine, or self-care queues at intake, and a wrong output — particularly a false negative on an urgent case — risks delayed emergency care to a patient, an outcome that is not reversible after the fact.
Assessor	Pulse Governance



1. EXECUTIVE SUMMARY

1.1 PURPOSE AND SCOPE

This gap assessment measures Patient Triage Assistant against ISO 42001 / NIST AI RMF / NIST CSF / SOC 2 / HIPAA / US State AI and Privacy Regulations / Workforce AI Governance and reports the distance between the two. It identifies gaps, prioritizes remediation, and sequences the work required to close them. It does not itself establish compliance, certification or attestation. Several of the frameworks assessed are management systems that an organization is certified against or attested to rather than compliant with, and any determination of that kind rests with the relevant auditor, certification body or regulator.

1.2 REGULATORY CONTEXT

Brazos Diagnostics is a HIPAA covered entity operating twelve clinics in Texas, so HIPAA's Security Rule, Privacy Rule, and breach notification obligations reach every system touching PHI, including the Patient Triage Assistant and the third-party AI assistant staff already use. Because all clinics and patients sit in Texas, the state's AI and privacy regime applies, including the Texas Responsible AI Governance Act's affirmative defense provisions tied to documented internal testing and NIST AI RMF alignment, and Chapter 181-Subchapter 118's biennial signed training obligation, both currently unmet. The compliance committee's own roadmap to renew the SOC 2 examination within twelve months brings the AI pipeline into that audit's scope, and NIST AI RMF and NIST CSF apply as the risk and security frameworks relevant to the (PHS-based) PHU (healthcare) production environment. ISO 42001 applies because the organization operates a production AI system requiring lifecycle governance even without pursuing certification. Workforce AI Governance applies because state law (workforce AI)

CONFIRMED GAP

CLIENT REPRESENTATION

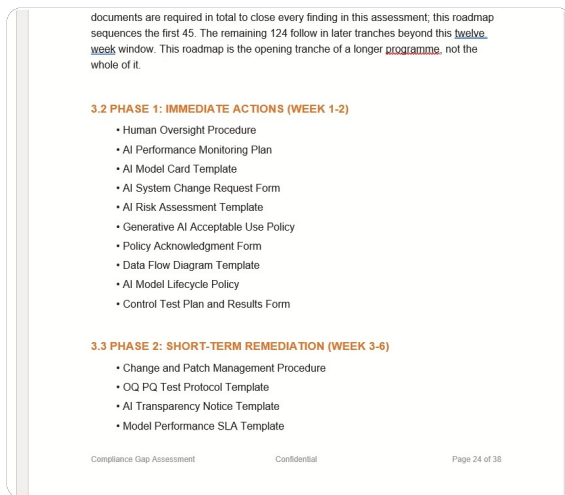
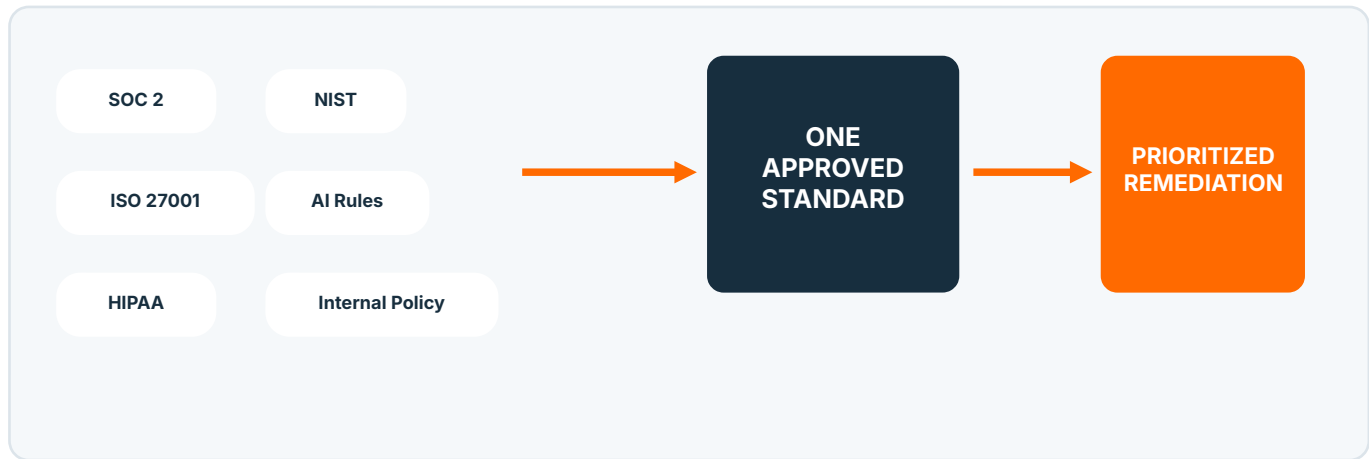
CANNOT ESTABLISH

The point is not the number 109. The point is knowing what matters first - and why.

STEP 4

Many frameworks. One closure path.

The practitioner does not hand the client 109 disconnected actions. The diagnostic shows where the same control or remediation closes exposure across several frameworks at once.



61 of 109

findings touched two or more frameworks in the synthetic example.

One remediation action can close exposure in several places. A long gap list becomes a sequenced set of actions.

The output does not say: 109 findings means 109 documents. It shows the smallest set of actions that addresses the greatest exposure.

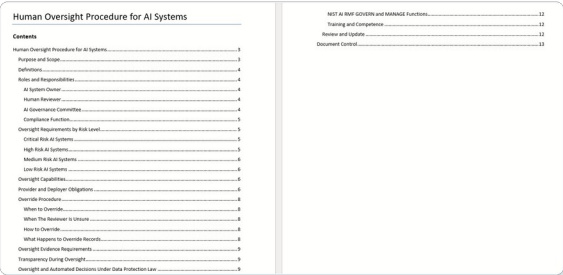
STEP 5

The output gets shorter because it gets smarter.

A generic template has to cover every organization that might need it. A fitted document removes what does not apply and preserves what reaches this client.

GENERIC TEMPLATE

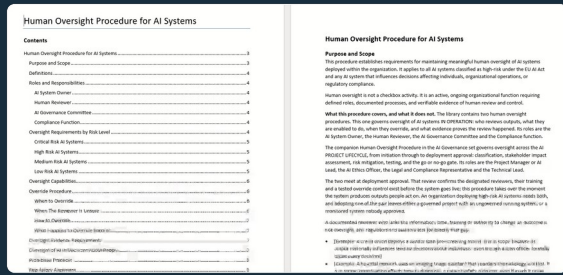
13 pages



Written to cover every organization that might need the procedure.

FITTED FOR THIS CLIENT

10 pages



Shorter because everything that does not apply to this organization is gone.

Policy generation is not new. The difference is what the generator was working from: the sector, jurisdictions, system, data, and findings.

The goal is not more paperwork. It is less irrelevant paperwork.

WHAT HAPPENS NEXT

The document is not the finish line.

The approved standard does not stop at documentation. It becomes the basis for testing whether execution actually matched intent.



Execution results can surface four different truths:

CONFORMED

DEPARTED

CANNOT ESTABLISH

NO GOVERNING RULE

Documentation tells you what should happen.

Execution Integrity shows whether it did.

The technology can accelerate the evidence path. The practitioner still owns scope, judgment, validation, and any professional conclusion.

A LOW-COMMITMENT NEXT STEP

See how Pulse works in 15 minutes.

You do not need to commit to the full journey. Start with a brief conversation to see the diagnostic output, understand what intake requires, and decide whether Pulse fits your current priority.

Talk to a Pulse Practitioner

See the diagnostic output, ask questions, and decide whether Pulse fits your current priority.

[TALK TO A PRACTITIONER](#)



Scan to talk to a practitioner



Edward J. Beltran, CPA

Chief Executive Officer, Fierce Inc. · Creator, Pulse Governance

Edward began his career in risk assurance at Arthur Andersen and PwC, focused on internal and systems controls. His work connects public accounting, enterprise operations, and the question at the center of Pulse: whether execution matches approved intent.

Built on more than 25 years of enterprise work through Fierce Inc., which has served more than 60% of the Fortune 500.

pulsegovernance.com

Find the gaps. Close the standard. Prove execution.