

Next Gen Compliance: Escaping the Evidence Avalanche

John Spisiak

VP, Security Compliance



Brigitte Calderon Vargas

Security Compliance Analyst



20 YEARS OF SECURING PAYMENT DATA

The Paradigm Shift

From Manual Evidence Chasing to Automated Evidence Orchestration



The Pain of Point-in-Time Audit Cycles

Why waiting for the audit window to collect, review, and upload evidence creates operational chaos



The Evidence Avalanche

Evidence Overload

Suddenly managing 100s of simultaneous evidence requests across people, processes and modern technologies.

Stakeholder Friction

Manually routing tasks to dozens of different team owners, then chasing them down across departments to meet strict deadlines.

Review Bottlenecks

SMEs waste hours manually evaluating every received artifact, checking for compliance gaps and ensuring quality for submission.

Swivel-Chair Uploads

Manually downloading files from internal systems, writing descriptions, and uploading them one-by-one into GRC platforms.

20 YEARS OF SECURING PAYMENT DATA PCI

The Next-Gen Compliance Blueprint

Transforming stale Business-As-Usual compliance into a continuous, optimized pipeline.

*Escaping the Evidence Avalanche requires a modern compliance blueprint: powered by **automation**, orchestrated by **AI agents**, and anchored by **human authority**.*

01

The Orchestration Layer

Automation as the muscle to collect and deliver evidence at scale (e.g., RPA, REST APIs, scripting, connectors, and Webhooks)

02

The Intelligence Layer

AI as the first-line analyst leveraging domain-tuned AI agents to execute artifact reviews, quality checks, and automated gap analysis.

03

The Integrity Layer

Humans as the authority to enforce Human-in-the-Loop (HITL) validation to ensure total accountability, capture operational context, and guarantee audit-grade integrity.

20 YEARS OF SECURING PAYMENT DATA PCI

The Orchestration Layer

Automation as the muscle of evidence collection



Automate & Orchestrate: Low-Code Evidence Collection

Deconstructing controls by System and Process, then Automate!

The Strategy (System vs. Process)

System Accessibility
Locating where technical proof-of-state natively lives (Cloud APIs, directory platforms, config files, SIEM database tables).

Process Workflows
Map out the human/operational approval loops (front-door tickets, reviews, change requests, access controls).

The Goal
Isolate repetitive, high-volume actions to automate up to 70% of collection without engineering dependencies.

5 Low-Dev, Tool-Agnostic Use Cases

1. **IAM & Entitlement Integration:** Replace manual spreadsheet checks by auto-extracting permissions from directory services to standardized lists.
2. **API-Driven Policy Validation:** Connect directly to infrastructure/WAF endpoints via API to output rules to a structured compliance validation matrix.
3. **Log Evidence Extraction:** Use RPA or saved queries in SIEM systems to pull required watchlist paths and host coverage logs into audit bundles.
4. **Logic-Matrix RPA Uploads:** Feed an evidence mapping spreadsheet to desktop RPA bots to automatically upload files and auto-fill GRC portal fields.
5. **RPA-to-AI Agent Routing Pipeline:** Deploy RPA to download raw evidence, reference the control framework number, and programmatically ingest artifacts into matching domain-based AI Agent directories.

20 YEARS OF SECURING PAYMENT DATA PCI

Evidence Collection Workflows

Logical Access Controls

IAM Platform Integration
Automates extraction from IAM platforms, replacing manual user list exports

↓

Entitlement Cross-Referencing
Validates individual entitlements against defined organizational scope

↓

Formatting & Standardization
Generates perfectly standardized, system-generated listings of permissions

↓

Instant Evidence Pipeline
Transforms tedious data-gathering into a streamlined validation process

WAF Policy Review

API Data Connection
Connects directly to policy report data to retrieve WAF status

↓

Python Validation Script
Cross-references hostnames, regions & policies with target list

↓

Data Filtering & Categorization
Sorts data into tables: "Blocking", "Transparent", or "Not Found"

↓

Report Generation
Automatically creates a formatted, structured PDF evidence report

↓

Evidence Submission
Final PDF report is processed and queued for portal upload

Log Evidence Extraction

RPA Extraction Workflow
Automatically executes queries directly in log management tools

↓

Watchlist Data
Extracts configured paths

Host Coverage
Pulls monitored host lists

↓

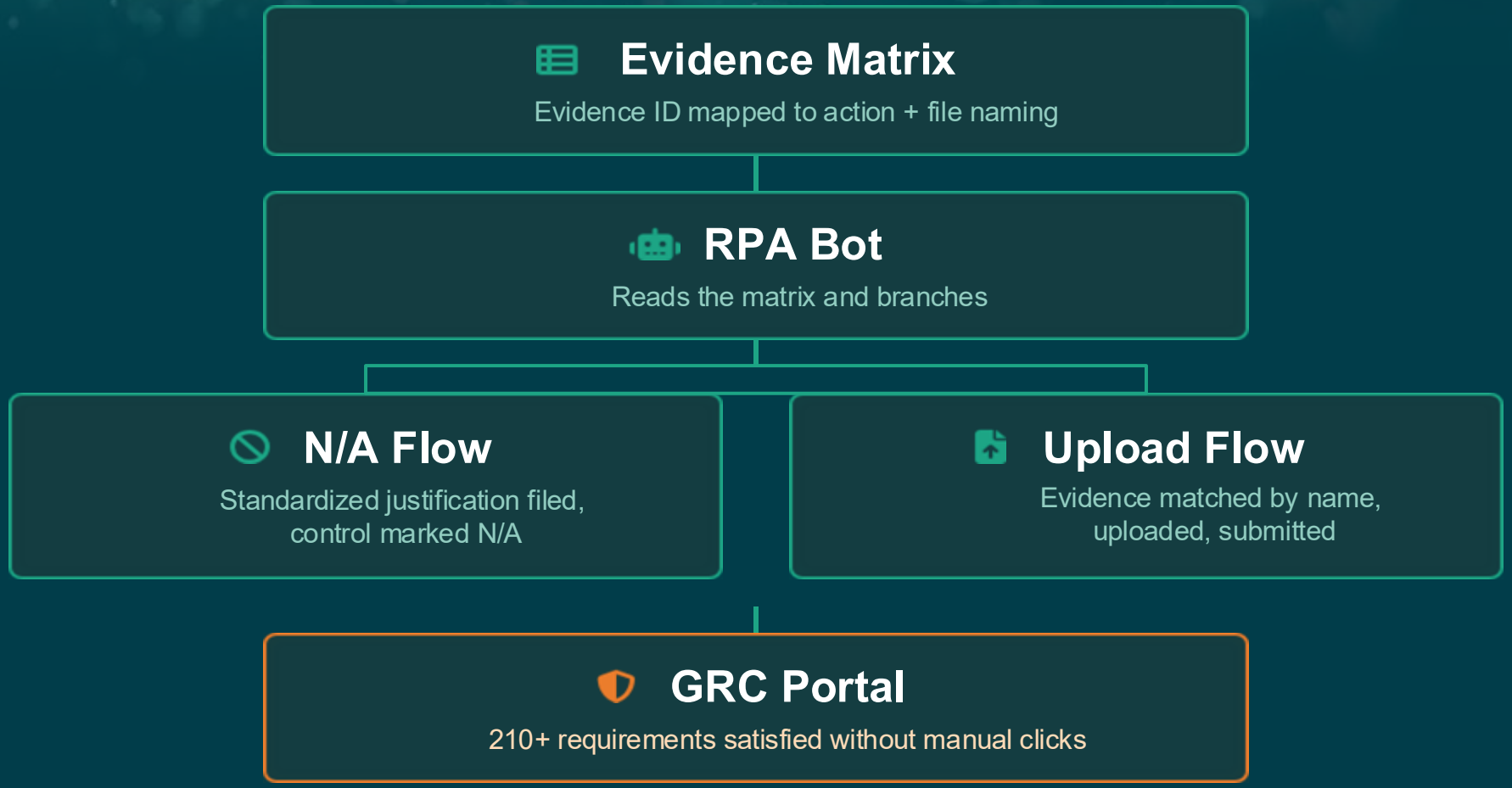
Standardized Evidence Output
Raw evidence is compiled into a clean, standardized format

↓

SME Validation
Analysts review hosts and verify incident responses without writing manual queries

Eliminated 100% of manual log querying for sampled applications

GRC Portal Evidence Task Automation at Scale



SMEs freed from data entry

~80% less upload time in our use cases

20 YEARS OF SECURING PAYMENT DATA PCI

RPA-to-AI Agent Routing Pipeline

RPA Extraction and Update

GRC Repository Download
RPA accesses the evidence locker and downloads evidence and request status matrix

↓

AI Agent Transmission
References the control # to an AI agent Directory and loads artifact into agent (domain-based)

↓

Analysis Extraction
Loads structured analysis (JSON) into validation sheet for HITL sign-off

↓

GRC Repository Reconciliation
Loops through requests post-validation to add comments and closure dramatically reducing clicks. Final PDF report is processed and queued for portal upload

↓

Evidence Reviews Complete

20 YEARS OF SECURING PAYMENT DATA PCI

The Intelligence Layer

AI as the analyst for high-cognition tasks



Gen AI Optimization of Reviews

Orchestration and Intelligence combined in one pipeline

01. RPA Feeds AI Agent

RPA extracts evidence and loads narrative descriptions and audit artifacts directly into the targeted AI agent directory.

02. AI Agent Analysis

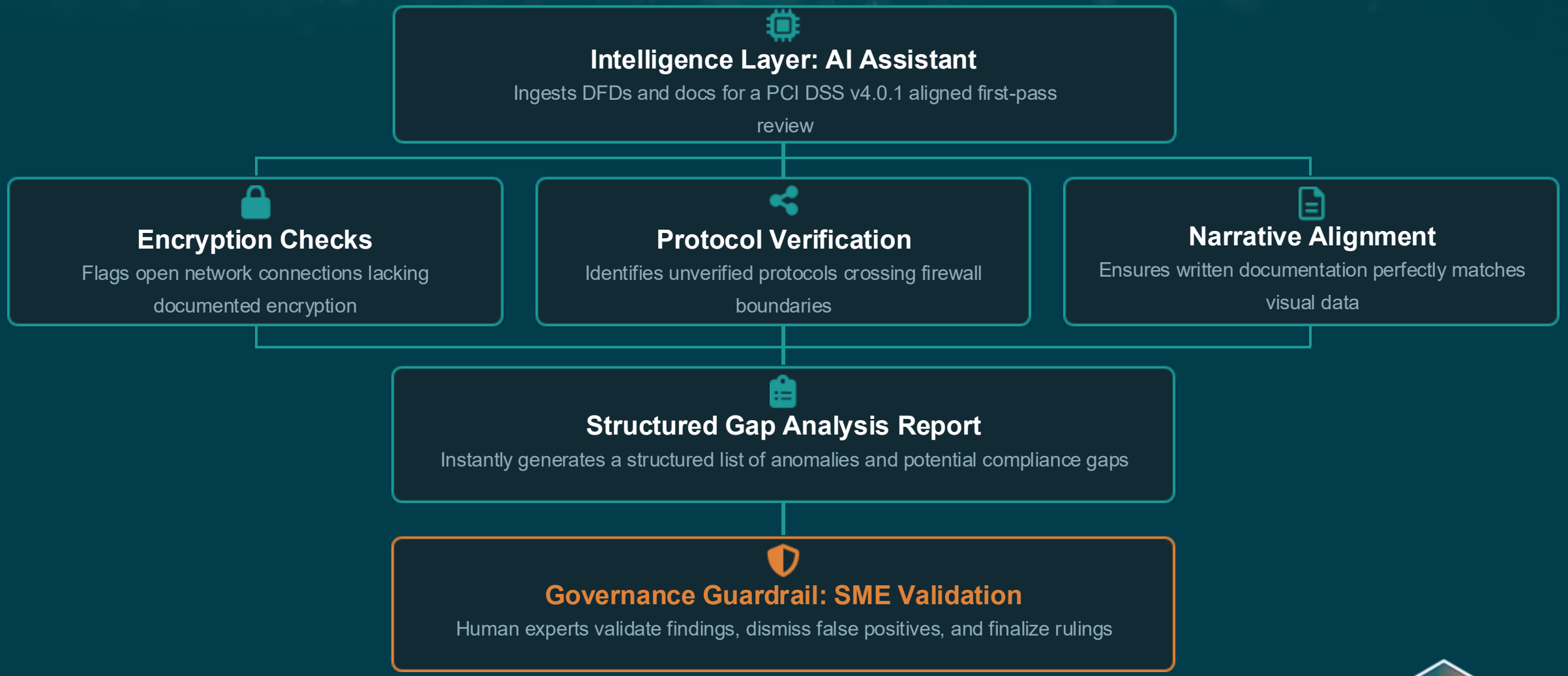
The specialized agent processes metadata, performs strict chain-of-thought analysis, and runs high-cognition compliance reviews.

03. SME Authoritative Sign-off

Human subject matter experts validate analysis, dismiss false positives, and provide authoritative sign-off under a zero-trust model.

20 YEARS OF SECURING PAYMENT DATA

AI-Automated DFD Review Flow



20 YEARS OF SECURING PAYMENT DATA PCI

AI-Assisted Pre-Assessments

Scope Applicability & Risk Assessment: AI prepares, your SMEs assess

Four inputs, one pass

Scope information, focus level, system description, and the previous cycle inputs (e.g., audit notes, transcripts, diagrams)

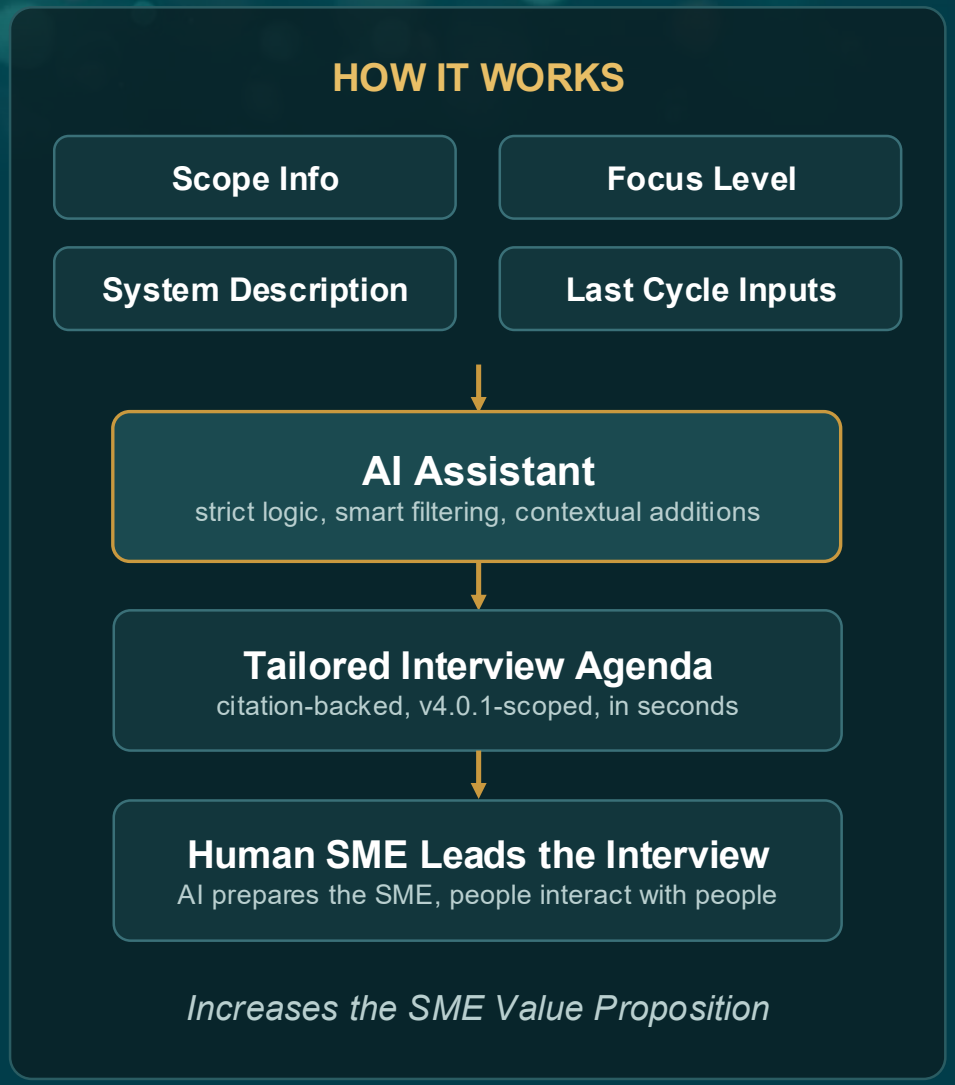
Strict scoping logic

Filters inherited requirements, injects suggested questions, converts open risks into follow-ups.

Human-led, always

Output is a citation-backed, v4.0.1-scoped agenda. The SME leads the interview; AI never conducts the assessment.

~90% less prep time in our use cases, improving pre-assessment quality



20 YEARS OF SECURING PAYMENT DATA PCI

The Pinnacle: Domain-Specific AI-Agent Reviews

Orchestration and Intelligence combined in one pipeline

01. Domain-Tuned System Prompt

Hardcodes specific framework text (e.g., PCI DSS), requirement IDs, and evidence criteria, establishing strict operational boundaries to prevent scope creep.

02. Forensic Metadata Gatekeeping

Programmatically scans artifacts for critical contextual markers (timestamps, hostnames, and user identities) enforcing recency, relevance, and attribution before evaluating content.

03. Chain-of-Thought Delta Analysis

Executes hidden, step-by-step cognitive evaluations, comparing observed technical configurations directly against framework compliance thresholds to isolate gaps.

04. Schema Enforcement & Citations

Forces output into a deterministic JSON structure with mandatory source references (source_reference), guaranteeing audit-grade provenance for human validation.



20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

The Integrity Layer

Human-in-the-loop governance



The Governance Guardrail

AI can hallucinate, so it never makes the final compliance ruling

01 The AI Core Team

A dedicated team serves as the human-in-the-loop authority, certifying every broad-use AI process before deployment

02 Secure Prompting (SHIELD)

Sanitized, Hyper-scoped, Insulated, Evaluated, Least-Privilege, Defensive Non-negotiable execution guardrails for secure prompt engineering and model training

03 A Gold Standard Workflow

Design principles, a technical review rubric, safe-harbor testing, and a final competency check with a live demonstration

04 Zero Trust for AI

No finding without a citation; ambiguous evidence is marked Inconclusive, never guessed



20 YEARS OF SECURING PAYMENT DATA PCI

Human-in-the-Loop by Design
The Interrupt Pattern

A decision-support system, never a decision maker

01 Interrupt

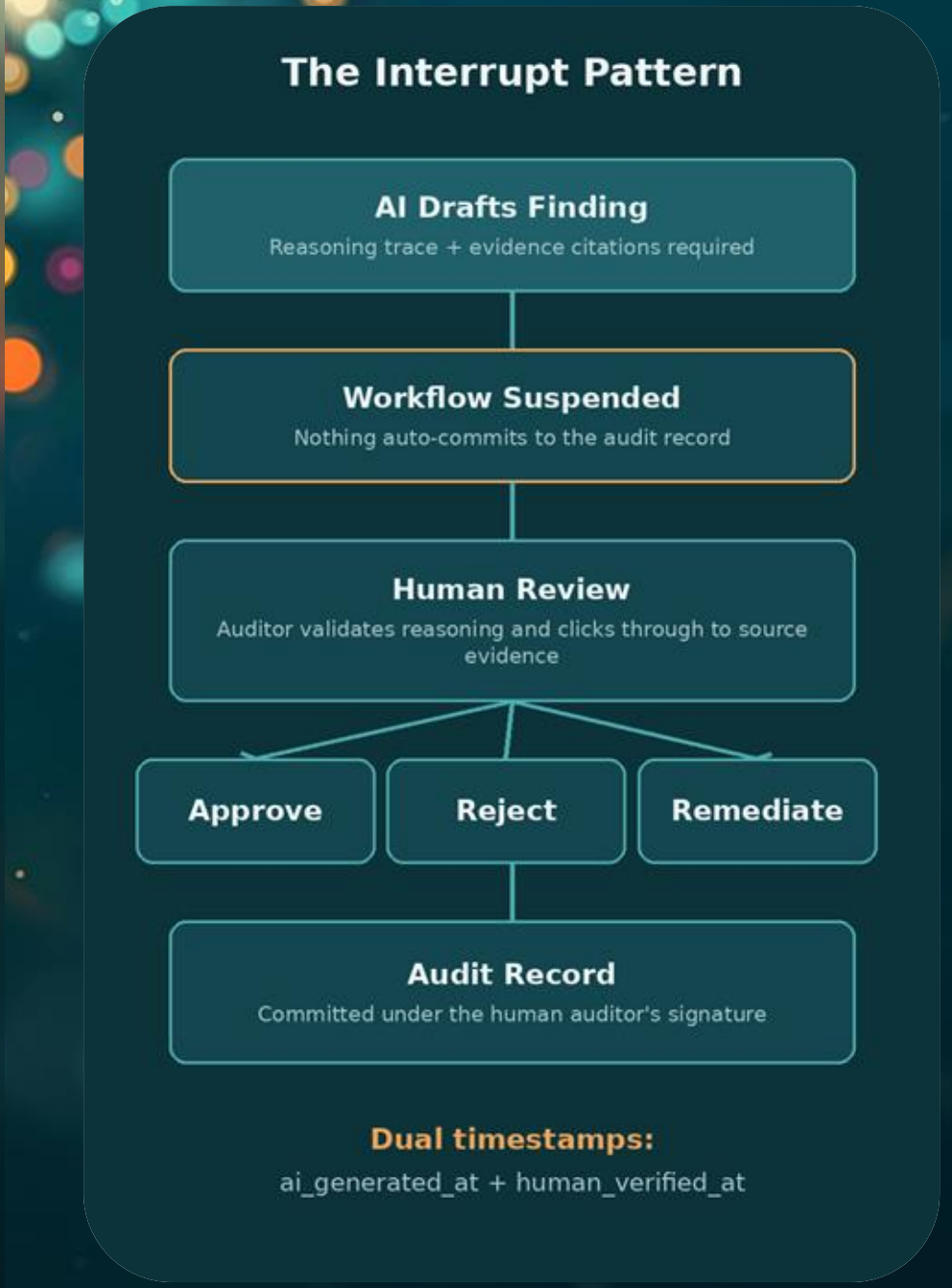
After the AI drafts a finding, the workflow pauses in a suspended state; nothing auto-commits to the audit record.

02 Validate

The compliance analyst reviews the reasoning trace, clicks through to the source evidence, then approves, rejects, or remediates.

03 Proof

Dual timestamps (AI-generated and human-verified) plus an evidence-first review flow that defeats automation bias.



Key Takeaways

Three blueprints you can take home

Continuous Pipeline

RPA, scripts, and workflow mechanisms that automate evidence collection and common audit tasks with direct GRC integration.

AI-Driven Review

Dedicated, requirement-tuned AI reviewers paired with automation for an end-to-end evidence aggregation and review lifecycle.

Governance Guardrail

An AI Core Team blueprint: mandatory QA, standardization, and human-in-the-loop validation for audit-ready integrity.

SME Empowerment & Human Authority

Human SMEs empowered as critical validators and decision makers serve as the final authority on compliance integrity. With automation handling the heavy lifting, they become more available for deep-dive discussions, proactive problem solving, and serving as strategic internal consultants to the business.

20 YEARS OF SECURING PAYMENT DATA PCI

Thank You

John Spisiak
VP, Security Compliance

Brigitte Calderon Vargas
Security Compliance Analyst

Connect with us on LinkedIn