



How AI is changing the TPRM operating model



Paul Valente, Co-founder and Chief Customer Officer

Vendor & Third Party Risk USA · TPRA + CeFPro · Fort Worth · October 14–15, 2026

Where programs stand in 2026

TPRM teams are small, portfolios are large, and work is backing up

63%

of programs run with
one or two dedicated
people

53%

manage 300 or more vendors

40%

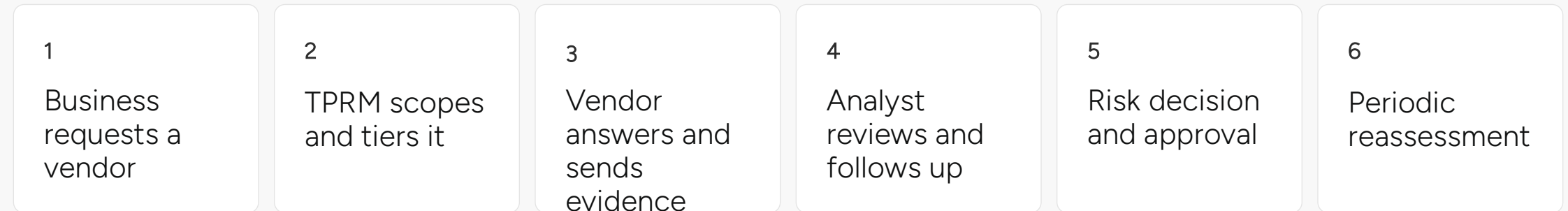


report a backlog of third-party
assessments

Sources: Ncontracts 2026 State of TPRM Survey (financial services); ProcessUnity and Ponemon Institute, 2026

The most common operating model today

Human-executed, questionnaire-centric, periodic



Software orchestrates the workflow. Humans perform the substantive due diligence.

The shift this talk is about

From human-executed TPRM to machine-executed, human-governed TPRM

AI can now perform the assessment.
Most programs are still designed around humans performing it.

Today

01 What AI in TPRM actually means

02 My story

03 Six years of AI in production

04 How the operating model shifts



01

What AI in TPRM actually means

The spectrum

"AI in TPRM" covers seven very different things

Conveniences

- Conversational help
- Regulatory guidance
- Artifact summaries
- Company research

Risky shortcuts

- Ungrounded questionnaire answers
- DIY AI risk assessment

Engineered agents

- Atomic agentic processes, evaluated continually by subject matter experts

Only the last one changes the operating model.

Conveniences

Useful, low risk, and no change to the operating model



Conversational help

Answers how-to questions about your tools



Regulatory guidance

Finds and explains guidance and best practice



Artifact summaries

Condenses a document without assessing it



Company research

General background on a vendor, not assurance

Risky shortcut 1

Ungrounded questionnaire answering produces confident answers with nothing behind them

On the vendor side

Vendors use AI to fill out trust questionnaires.
Often the model is simply writing plausible answers.

On your side

You receive fluent, complete answers.
Nothing tells you which ones are true.

A well-written answer is not evidence.

Risky shortcut 2

A DIY AI risk assessment piles approximation on assumption on hallucination



No framework

No defined controls or criteria behind the judgment



Not deterministic

Ask twice, get a different result every time



Hallucinates

Invents certifications, controls, and facts



Brand bias

Well-known names get the benefit of the doubt

Engineered agents

Atomic agents do one job each and are evaluated continually by qualified experts



Live agentic research

Collects what is public about a vendor, as it changes



Deep evidence analysis

Reads artifacts the way an auditor does



Interactive platform agents

Do the program work around the assessment

Live agentic research

Research agents build the picture before anyone sends a questionnaire

Risk advisory collection	Breaches, incidents, disclosures, and news
Public artifact collection	Policies, privacy terms, and documents vendors publish
Compliance badge collection	The certifications a vendor claims, and what they imply
Trust portal analysis	What is available, what is gated, and what is current
Use case and context prediction	Likely use, data involved, and inherent risk

Deep evidence and artifact analysis

Each type of artifact gets its own specialized agent

Retrieval-augmented generation and vector search, built and maintained by AI engineers

SOC reports

ISO statements of applicability

HITRUST reports

Penetration tests

Policies

Data flow diagrams

Financial statements

Service level agreements

Privacy terms

Deep evidence and artifact analysis

Inside each artifact, agents check what an auditor checks

Control language

Does the control exist as described?

Test language and assurance

How was it tested, and by whom?

Exceptions

What failed, and does it matter to you?

CUECs

What does the vendor expect you to do?

Subservicers and subprocessors

Who else is in the chain?

Dates, locations, validity

Is it current, and does it cover this service?

Interactive platform agents

Platform agents do the program work around the assessment



Summarization and reporting

Program and board views on demand



Ad hoc analysis and communication

Ask a question across the portfolio, draft the response



Long-running tasks

Work that spans days and many vendors



Vendor collection and intake

Agents request, collect, and log what is needed

The difference

The difference is in the engineering

	DIY AI	Atomic agents
Framework	None	Explicit, any framework
Repeatability	Different result each run	Consistent and measured
Grounding	Model memory	Cited evidence
Bias	Brand reputation	Artifact content
Oversight	None	Continual expert evaluation

02

My story

My story • Before VISO TRUST

As CISO at LendingClub, I had to keep pace with aggressive growth

4,000+

vendors the company relied on
as it matured

CISO at several companies before co-founding VISO TRUST

New vendors had to be onboarded quickly to support growth initiatives

Third-party risk was a board-level priority

My story • What broke

Our "lightweight" questionnaire process was slow and labor intensive

Vendors failed to respond

Procurement was delayed

Stakeholder frustration went through the roof

We were labeled the department of no.

Accused of killing innovation and getting in the way of delivering value to customers.

My co-founder Russ Sherman and I knew there had to be a better way

What we found

Every tool on the market was built to prove a program existed, not to reduce risk.

What it had to be

Evidence-based, using the evidence vendors already have.
Easy and fast for vendors, so visibility could scale.

The bet

Evidence-based, AI-powered assessment. A patented approach. Out of stealth in 2020.

Critical security advisory

Just now

Delayed Token Expiry Detected in
ACME Inc. Internal Environment

Risk increased from **High** to **Extreme**

VISO TRUST has analyzed ACME's security artifacts and identified
20 test failures and gaps in audit documentation.

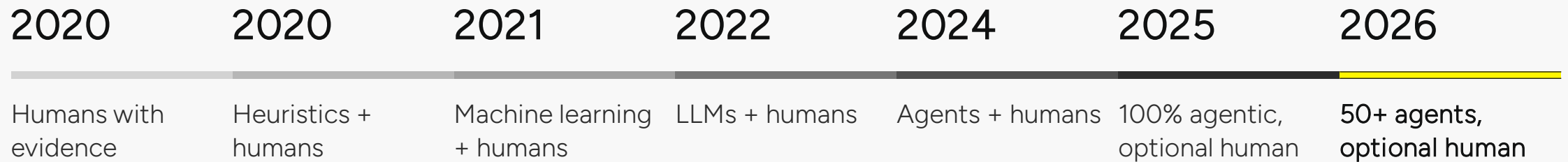
Take action

03

Six years of AI in production

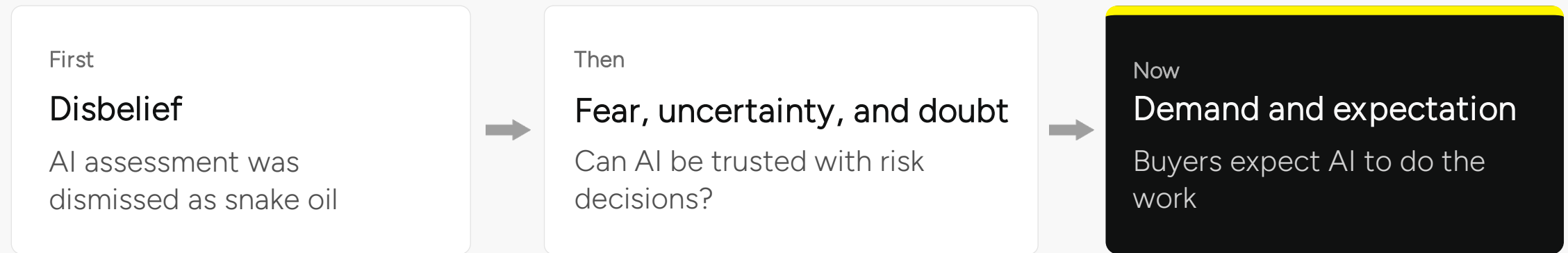
The VISO TRUST AI journey

Each generation moved more of the work from humans to machines



How the market responded

The market moved from disbelief to demand



The human role

Experts now evaluate the agents instead of reviewing every output



Credentialed auditors tune the system

CISSP, CISA, CISM, CTPRP, ISO 27001 Lead Implementer, and Big Four audit experience



Quality is measured continuously

An AI evaluation system, routine QA measurement, and human spot checks



Human review is a choice

Available on any assessment, every time if you want it. Not the default.

50+

specialized AI agents in production in
2026



Live agentic research



Evidence and artifact analysis



Interactive platform agents



[Other category, e.g. monitoring]

Delivered in production

90,142 assessments across about 120 organizations

3.6M

hours of senior analyst work saved

\$250M

in analyst cost saved

\$2.1M

saved per organization

About 40 hours saved per assessment, valued at \$69.37 per hour:

US average total pay for a senior vendor risk analyst (\$144,283, Glassdoor, 2026) over 2,080 hours.

Our customers

Trusted across financial services, insurance, healthcare, and technology





04

How the operating model shifts

Operational shifts

Seven shifts in how TPRM operates

- | | | | |
|---|-----------------------------|---|---------------------------|
| 1 | Faster | 5 | Engaged business owners |
| 2 | More efficient | 6 | One integrated tool |
| 3 | Evidence-based | 7 | A smaller, strategic team |
| 4 | Beyond "data plus workflow" | | |

Shift 1 • Faster

TPRM stops being the reason procurement waits



Fewer losses from delay

Projects and deals stop stalling while an assessment waits in a queue



A better friend to the business

Business owners bring vendors to TPRM early instead of working around it

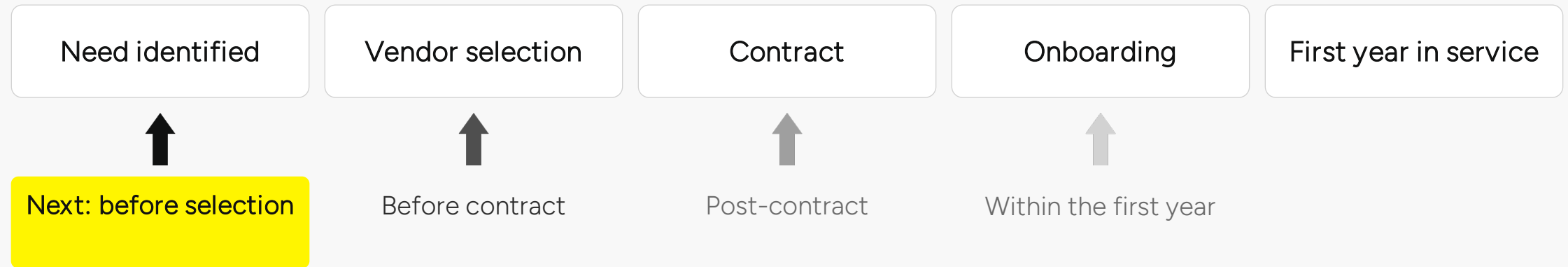


Room to move earlier

When an assessment takes minutes, it can happen before decisions are made

Shift 1 • Faster means shifting left

Assess while the decision is still open



Assessed just before signing, or after, the vendor is already chosen. The review becomes a formality.

Shift 2 • More efficient

Cover every vendor, not only tiers 1 and 2

Step 1

Start from what is public

Initial assessment from public artifacts and what a vendor's badges make likely

Step 2

Know the risk at intake

Use case and inherent risk determined instantly

Step 3

Cover the long tail

Significant risk sits in lower tiers too

Move off questionnaires and onto evidence

Questionnaires

- Slow
- Painful for both sides
- Subjective
- Often never answered

Evidence

- Quality: defensible and accurate
- Speed: no waiting on answers
- Breadth: more relevant detail

Shift 4 • Beyond “data plus workflow”

The “data plus workflow” model is coming apart

Workflow tools, data feeds, and outsourced services **consolidate into one agentic function.**

Workflows that took experts months to configure are no longer necessary

- ✓ Any framework, or all of them. No more choosing, mapping, rationalizing, and configuring.
- ✓ No large, complex team or process. Less outsourcing.
- ✓ No more paying to have artifacts reviewed.
- ✓ No more paying to chase vendors.
- ✓ No more paying to analyze questionnaires, cross-reference, and follow up.

Six impact vectors, each driven by a few facts about the relationship

Data sensitivity

Data types and record volume

Operational criticality

Business criticality and substitutability

Regulatory exposure

AI decisions, data subjects, cross-border transfer, physical supply

Financial exposure

Role in financial reporting and transaction exposure

Downstream reach

How far the relationship extends downstream

Ethical and reputational

Physical supply chain

Ten risk dimensions, scored through those impact vectors

Risk dimension	Data sensitivity	Operational criticality	Regulatory exposure	Financial exposure	Downstream reach	Ethical and reputational
Information security	•	•			•	
Data protection and privacy	•		•		•	
AI governance	•		•		•	•
Fourth party and subcontractor	•	•				
Operational resilience		•		•	•	
Financial viability		•		•		
Product security		•			•	
Governance and ethics			•	•		•
Sanctions and trade			•			•
Sustainability and human rights			•			•

Data stops being a separate product

Adverse media is a feature

News and incident collection is one agent's job, not a separate tool to buy

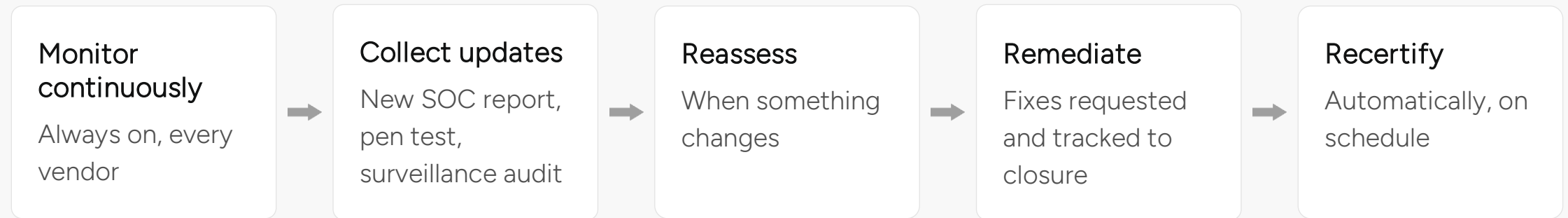
Monitor what you will be asked about

Status pages, disclosures, filings, and news you are expected to act on, in place of outside-in scans full of false positives

Point-in-time exchanges are dead

Agents gather the data in real time instead of from a shared, aging copy

Lifecycle management becomes fully automated



Vendor interactions happen automatically. No analyst sends the reminder email.



Shift 4d · Fourth and nth parties

Nth-party monitoring finally becomes operational

- Mapped automatically. Supply chains built from subservicer detections in vendor artifacts.
- Monitored across every party. Agentic monitoring gathers risk advisories up and down the chain.
- Answered by agents. Response flows act on an event as soon as it surfaces.

Business owners engage from day one. Experts join only where needed.

Top priority

Business owner engagement

- Intake in the business owner's own words
- Use case and context predicted, not interrogated
- Status and answers without chasing TPRM

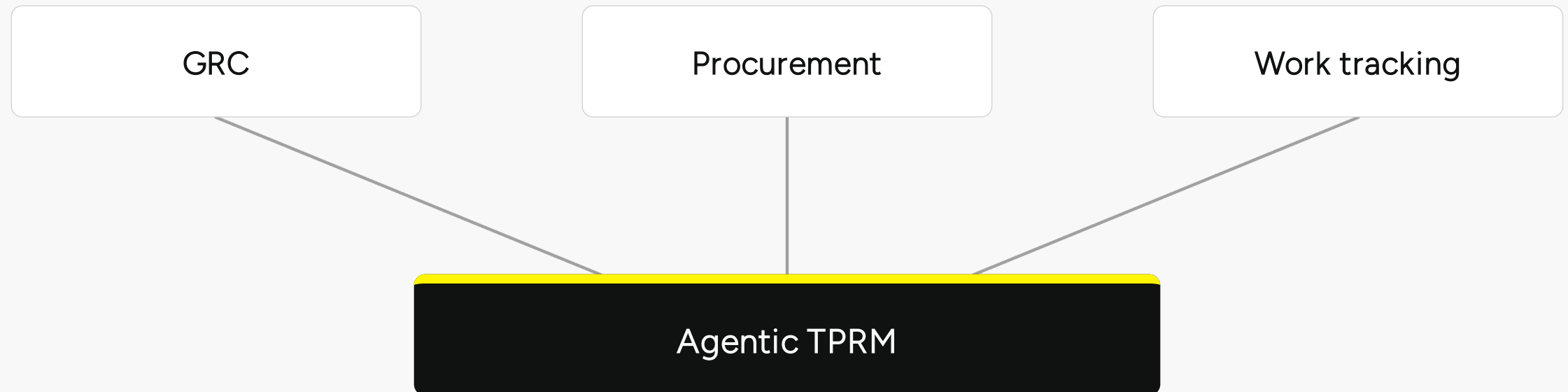
Where necessary

Easy SME interaction

- Privacy, legal, security, or AI governance pulled in on specific findings
- The evidence and context arrive with the request
- No routing every vendor past every expert

Shift 6 • One integrated tool

One agentic tool, integrated with the systems the business already runs



Shift 7 • A smaller, strategic team

The team gets smaller, better informed, and more strategic

	Today	The new model
Team	Large, with outsourced reviews	Small and focused
Technology	Disconnected tools	Fully integrated
Information	Point in time	Real time
Seen as	A drag on the business	A trusted partner
Contributes	Approvals	Better decisions and business value

TPRM that **strengthens business initiatives** instead of slowing them down

Strategic in helping the company achieve its goals and fulfill its mission.

Thank you

Paul Valente · paul@visotrust.com

Questions