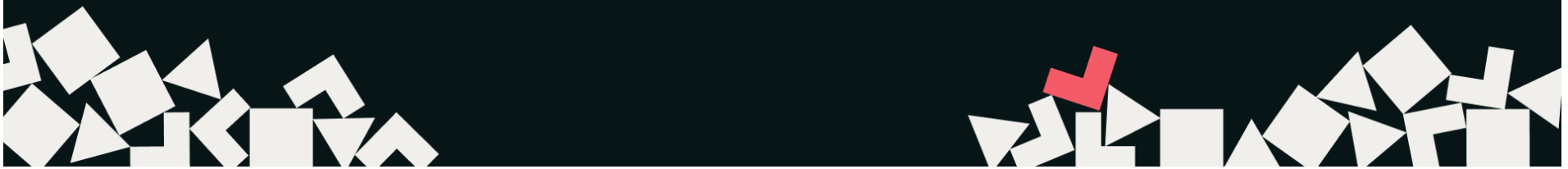
lema

The Vendor You Approved No Longer Exists

Johann Quiroz · Sr. Technical Sales, Lema

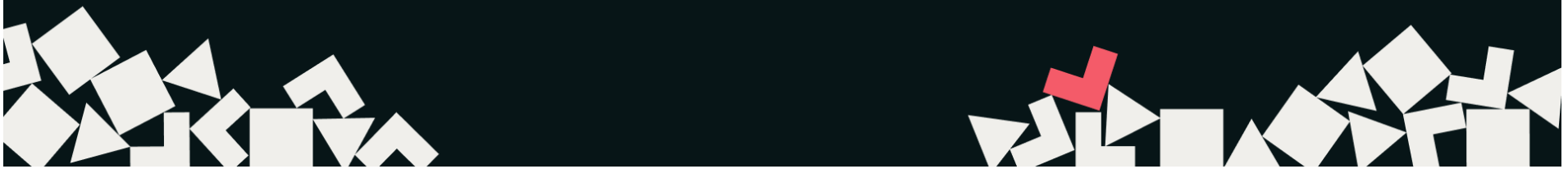


lema

THE GOVERNANCE GAP

Approval Captures a Moment in Time

The vendor keeps evolving. The approval record doesn't.




Ahh, now, are you going to go ahead and have those TPRM reports for us this afternoon?
lema

lema

THE PROBLEM

Today's TPRM Is Broken

Point-in-time
Reviewed once a year. Risk changes daily.

No business context
Every vendor gets the same review.

Compliance, not action
Collects documents. Rarely reduces risk.

30% of breaches involved a third party
Verizon 2025

$4.9M avg. cost of a third-party breach
IBM 2025

286 vendors per company
Whistic 2025

> **"Compliance shouldn't be the goal.** Understanding how a third party could break your business should." — Andy Ellis

THE STARTING POINT

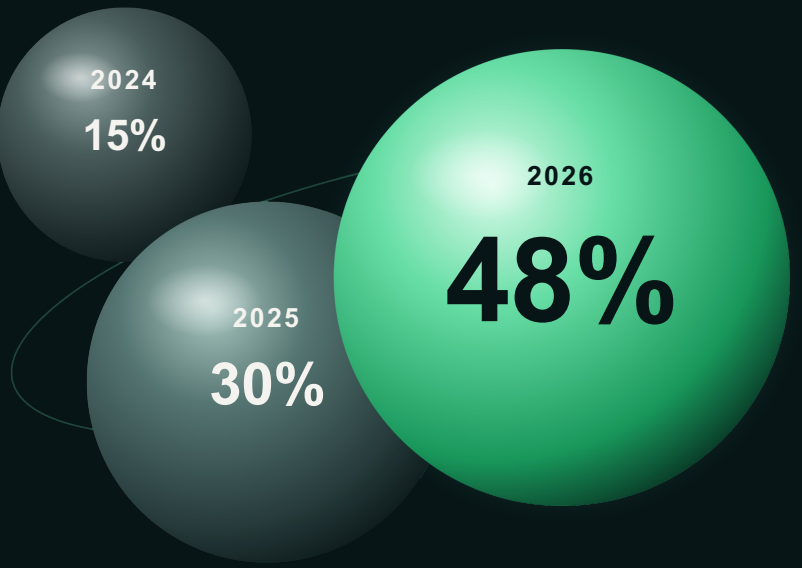
Why TPRM Exists

Your risk boundary extends
Their environment becomes part of yours.

Pressure comes from everywhere
Fourth parties, regulators and plain vendor failure.

Point-in-time doesn't hold
One question, answered once.

"Trust your vendors, but Verify, and then verify again!"



of breaches now involve a third party
Source: Verizon 2026 Data Breach Investigations Report

lema

ONE VENDOR, TWO STATES

The Vendor Changed. The Workflow Didn't.



THE ONBOARDING PROBLEM

Vendor Onboarding Is Like Speed Dating

ON THE DATE

“Oh, I'm totally low risk.”

- ✓ Works out daily
- ✓ Eats clean
- ✓ Encrypted at rest
- ✓ Never had an incident

5 MINUTES · NO EVIDENCE

AFTER YOU MOVE IN TOGETHER

“Okay, so about that…”

- ✗ Fridge full of unpatched servers
- ✗ A “just friends” list of 37 subprocessors
- ✗ Your data's been out with “a few close partners”
- ✗ Can't keep the place clean

3-YEAR CONTRACT · SIGNED

CASE 1 · DEFAULT BEHAVIOR CHANGE

One Feedback Click, One Exposed Conversation



01 SHIPPED DEFAULT

Rate chats on by default

Disclosed only in a privacy policy update.



02 USER ACTION

An employee rates a reply

While working with sensitive material.



03 CONSEQUENCE

Whole chat saved as Feedback

Data leaves the environment without any notification



04 CONTROL ACTION

Disable Rate chats

Admin setting under Data and Privacy.



One ordinary click changed how the entire conversation is treated.

CASE 3 · VENDOR EVOLUTION

Dialpad: AI Training by Default

APPROVED AS

Cloud phone system

For customer service calls.

ADDED SINCE APPROVAL

Call recordings and transcripts train AI models by default

New offshore subprocessor, with no contract change

The fix: turn off model training in Dialpad Admin.

CASE 4 · SCOPE DRIFT

5 Approved Users Became 116 Endpoints

APPROVED SCOPE · TPRM RECORD

5
ML users

10
endpoints

Offline. No customer data.

CROWDSTRIKE INVENTORY · REALITY

83
users

116
endpoints

23
internet-facing

38
vulnerable builds

18
in RCE range

Case 5:US Sanctioned vendor 1260H list

A Hidden Modem on New Laptops



01 SIGNAL

EDR sees every laptop

Read-only EDR data you already have.



02 FINDING

A modem nobody assessed

Quectel modem on 55 new Lenovo laptops.



03 EXPOSURE

A path around your controls

Over-the-air firmware on a link that skips the firewall.



04 FIX

Cut the path

Disable the modem. Confirm in CrowdStrike.



The takeaway: a vendor on the Pentagon's Chinese military list skipped procurement. It came preinstalled.

lema

A DIFFERENT QUESTION

Measure Exposure, Not Odds

THE USUAL QUESTION

How likely is an incident, and what would it cost?

LEMA'S QUESTION

What is our actual exposure?



What you approved

Scope, questionnaire, DPA terms



How teams use it

Data, permissions, OAuth, integrations



What breaks if it fails

The blast radius



Alerts follow your exposure, not just their posture.

TWO PLACES RISK HIDES

Rely on Real Evidence. Govern the AI.

FORENSIC ARTIFACT ANALYSIS

Extraction automates the checkbox. Lema questions it.

- Checks claims against their artifacts
- Flags every contradiction
- Confirms which product each artifact covers

THIRD-PARTY AI GOVERNANCE

Find the AI behind your vendors, approved or not.

- Which model providers sit behind them
- What that AI can read and act on
- AI added after approval
- Changes to model-training clauses

HOW LEMA GOVERNS VENDOR AI

Third-Party AI Governance



01

Discover

All AI, approved or shadow



02

Classify

What it is, does, and can reach



03

Map

Model providers and fourth parties



04

Assess

AI controls, claims checked against evidence



05

Monitor

New AI, AI risk, and scope drift



Something changes? That vendor's assessment reopens now, not at the annual review.

OWNERSHIP AFTER APPROVAL

Where Governance Gaps Live



01 INTAKE

Procurement

Knows the purchase.



02 CONTRACTS

Legal + privacy

Knows the terms and subprocessors.



03 RISK

Security + GRC

Knows the assessed state.



04 OPERATIONS

Technology owners

Knows what the vendor actually touches.



The gap: change signals fall between owners. No one reopens the decision.



What scares you the most?

"Werewolves!"

— Mike



What scares you the most?

"Vampires!"

— Nicki



What scares you the most?

"That companies are **NOT** using adaptive scoping, are **NOT** assessing real risks with evidence, and are **NOT** continuously monitoring for material risks when assessing or onboarding their third parties!"

— David



What scares you the most?

"David."

— Mark

lema

A PRACTICAL MATERIALITY TEST

Five Questions for Any Vendor Change

1	**What changed?**	New capability, policy, subprocessor or default
2	**What can the vendor reach?**	Permissions, identities, integrations, endpoints, cloud
3	**Has data use changed?**	Purpose, retention, training, location, sharing
4	**Did a control assumption change?**	Do the original evidence and controls still hold?
5	**Who owns the decision?**	An owner, an action, a deadline

MONDAY-MORNING ACTIONS

Start Narrow and Defensible



01

Pick ten critical vendors

Sensitive data, privileged access, or fast AI change.



02

Define material change

What reopens a decision, and who acts on it.



03

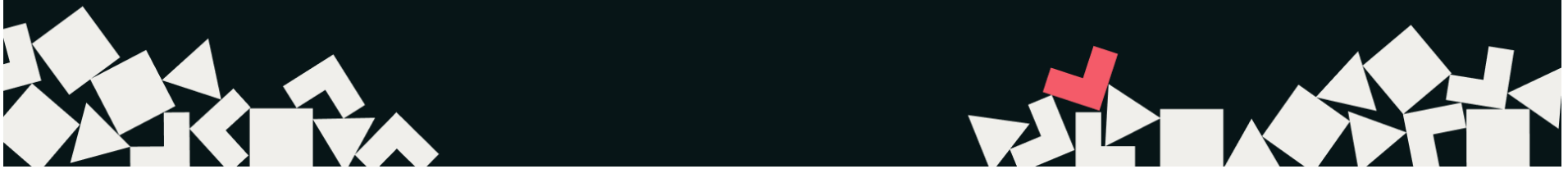
Connect one internal signal

Identity, endpoint, cloud or integration data you already have.

lema

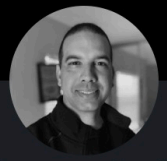
“The question is no longer whether you trust your vendors.

It's how they've changed since you last trusted them.”



lema

Let's Connect



Johanns Quiroz
Sr Technical Sales Southeast



Lee Cherry
Cybersecurity Sales Executive | IT Sales Executive | Start-up Sales Executive | GTM Sales Executive | En...