Modernizing TPRM

Strengthening Third-Party Compliance with AI and Automation

Aaron Wright
SecurityScorecard

Hassan Mahmoud
SecurityScorecard

Agenda

1. Why ‘Compliant’ vendors still create incidents
2. Defining ‘Continuous TPRM’
3. The Convergence of Compliance and Risk Reduction Through AI and Automation

Escalating risk.
Escalating scrutiny.

70%
of organizations will face increased scrutiny of their third-party risk programs

Third-party involvement in breaches doubled from
15% to 30%

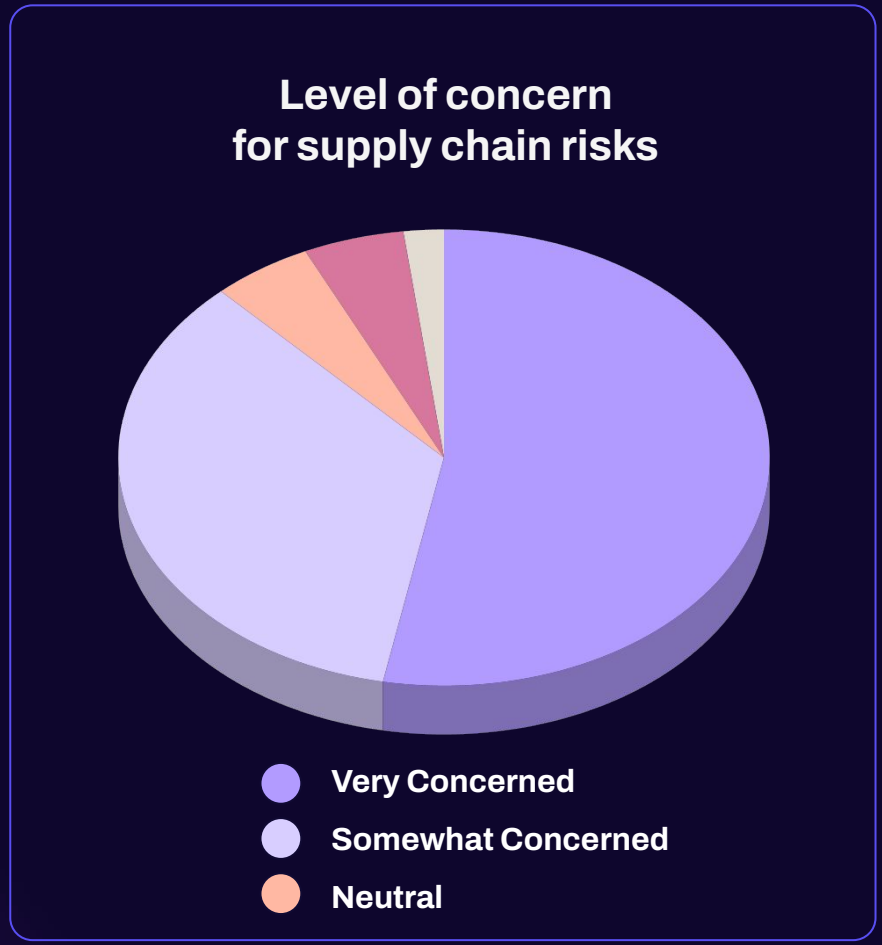
Your third parties are the new perimeter.

But most programs still run on quarterly evidence cycles.

Cybersecurity leaders:

So why are they so concerned about supply chain risks?

- **Vendor ecosystems change weekly** (access, tools, dependencies)
- **Evidence is point-in-time** (SOC2 PDFs, questionnaires, screenshots)
- **Risk is continuous** (control drift, exposed services, compromises)
- **Result: high effort, low signal, slow response**




COMPLIANC
E
RISK


RISK
COMPLIANC
E

FRAMEWORKS
REGULATIONS
MANDATES

What's the difference?

What's the difference?

FRAMEWORKS

Guidelines or blueprints for implementing cybersecurity controls

Examples:
NIST Cybersecurity Framework (NIST CSF) and the CIS Controls help organizations understand their cybersecurity posture by offering a roadmap for assessment and control prioritization.

REGULATIONS

Industry-specific and often enforce compliance with specific cybersecurity controls. Failure to comply may result in penalties or fines.

Examples:
GDPR, HIPAA Security Rule, SEC cybersecurity disclosure rule, DORA, NIS2.

MANDATES

Legally enforceable requirements, often set by national authorities, to protect data or respond to incidents

Examples:
- SEC material incident disclosure timelines and governance reporting
- GDPR breach notification timelines
- DORA requirements for ICT third-party oversight
- NIS2 incident reporting obligations

Future-Proofing

Despite the complexity, regulations are converging on three core requirements

Continuous monitoring

Moving beyond the "point-in-time" static audit. The security posture must be addressed daily and continuously.

Third-party inclusion

Mandates are increasingly highlighting the need for organizations to monitor third parties as part of their digital ecosystem

Prioritized, Evidence-Based Reporting

Organizations must prove how vulnerabilities are ranked based on the potential risk they pose, requiring irrevocable evidence. This is essential for communicating the effectiveness of controls to boards and regulators.

Future-Proofing

1. Vendor inventory and tiering
2. Risk based due diligence
3. Continuous monitoring
4. Incident response and escalation for vendors
5. Recovery and resilience validation

NIST CSF Maturity Tiers for C-SCRM

4 Adaptive
Fully institutionalized, real-time C-SCRM program. Positioned to lead with predictive insights, automation, and ecosystem-wide collaboration.

3 Repeatable
Beginning to build awareness of supply chain risk. Laying the foundation for visibility and discovery across the vendor ecosystem.

2 Informed
Developing structured practices for identifying and assessing vendor risk. Positioned to formalize vendor tiers and monitoring strategy.

1 Partial
Beginning to build awareness of supply chain risk. Laying the foundation for visibility and discovery across the vendor ecosystem.

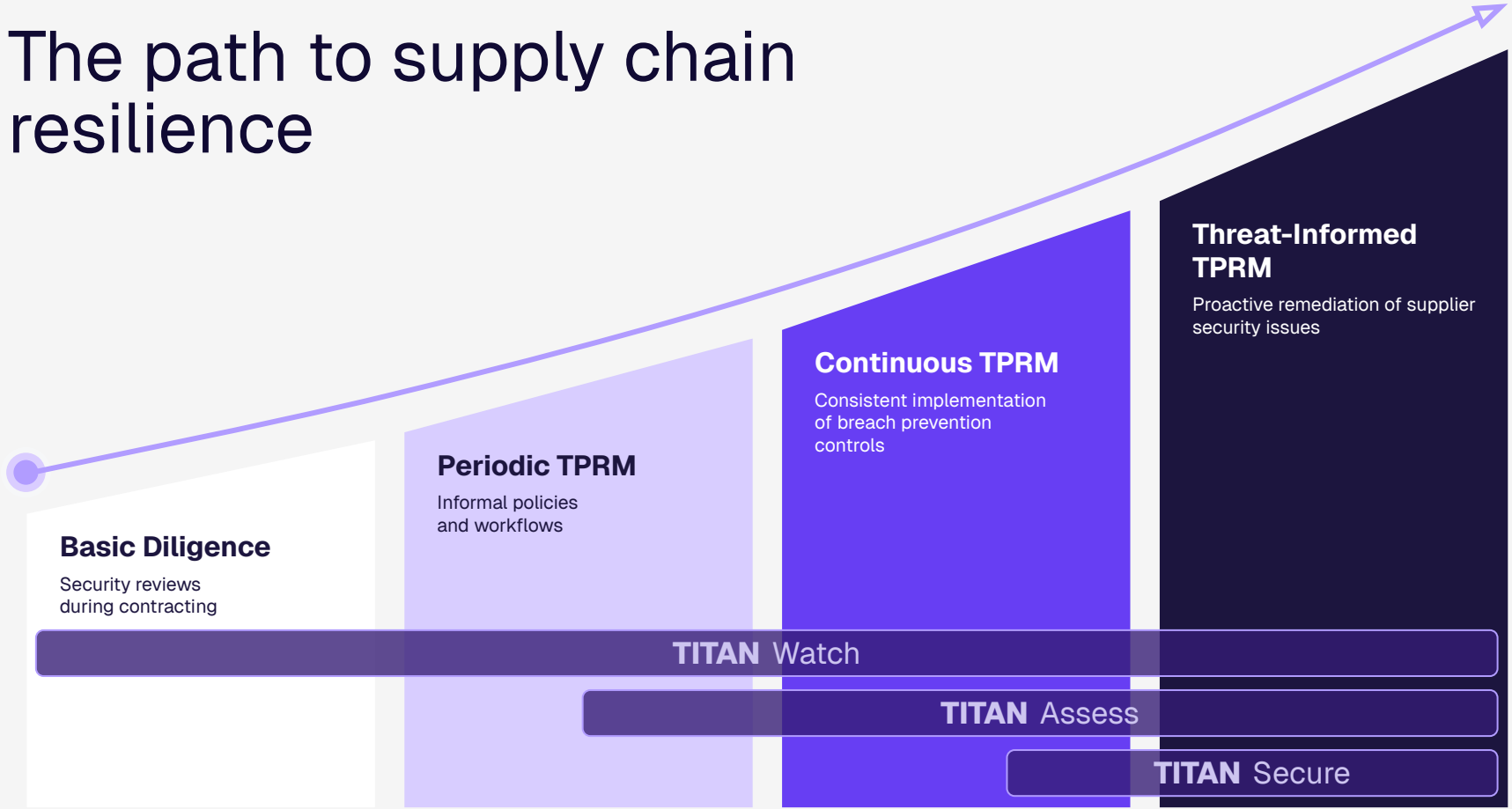
Note: The NIST Cybersecurity Supply Chain Risk Management Tiers are aligned with the NIST CSF 2.0 tiers. This alignment is helps to establish a common maturity language across cybersecurity and third-party risk management (TPRM) teams

Compliance is the minimum bar.
Risk reduction is the objective.

Compliance	Risk reduction	Where programs fail	The goal
Point-in-time proof (policy, regulator, contract)	Continuous identification, mitigation, and resilience	Optimizing for *document collection* over *control effectiveness*	Compliance artifacts as a byproduct of a working risk program


Continuous Monitoring
Always-on signals (outside-in posture, exposure changes, events)
Continuous TPRM
Monitoring +
Decisioning & Action:
Tiering and ownership
Workflows and escalation
Remediation tracking and proof
Offboarding and resilience planning
Executive reporting

The path to supply chain resilience

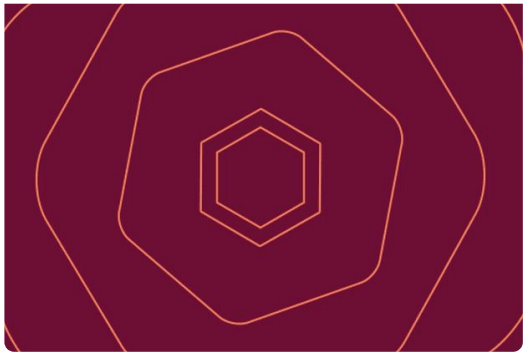


The automation stack

How you get both compliance *and* risk reduction.

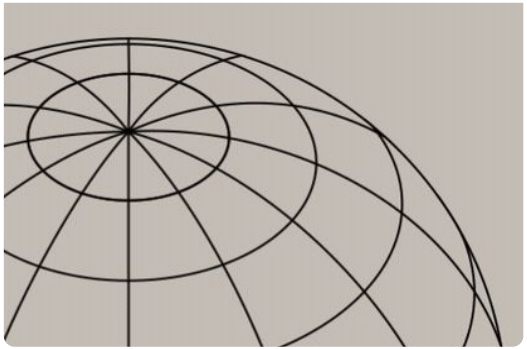
Evidence

- ingest artifacts and normalize
- AI-assisted mapping to your control language
- gap detection routed to owners



Monitoring

- posture and exposure changes
- event and incident signals
- tuned thresholds by vendor criticality

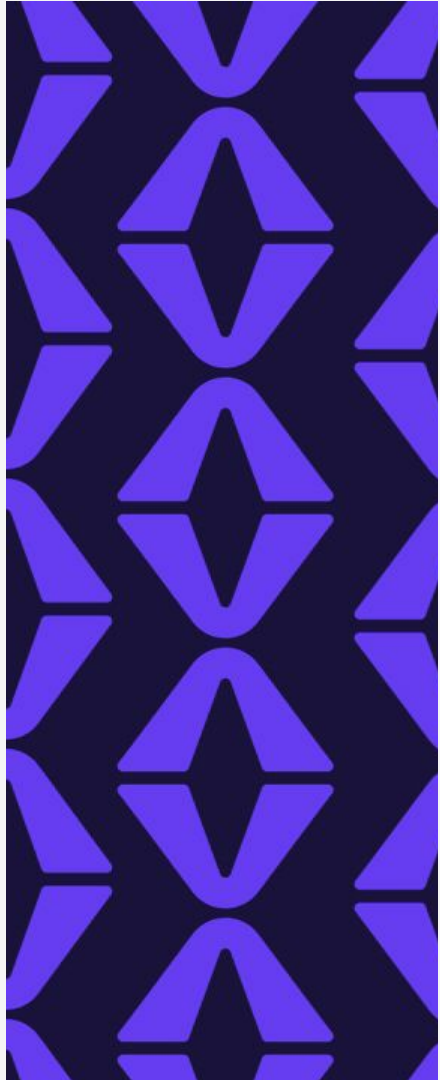


Response

- assign, escalate, and track remediation
- require proof and time-bound SLAs
- align decisions to business impact

What “action-driven” looks like (trigger playbook)

Trigger	Material posture drop or new critical exposure
Automated actions	• Notify vendor owner and security • Open ticket with required evidence and deadline • Escalate if vendor is critical or exposure is high • Update executive view of exposure and risk acceptance
Human value	Judgment, negotiation, and exceptions



The “overlap zone” is where programs scale.

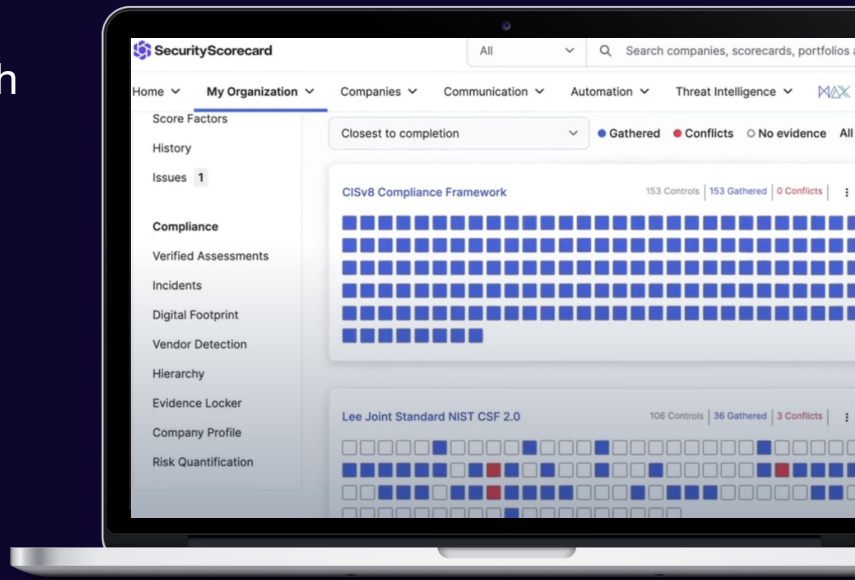
Continuous signals to reduce blind spots in between audits

Evidence and **control mapping** to reduce low-signal manual work

Workflows that drive **remediation and proof**, not just collection

Optional managed support when bandwidth is the constraint

Integrates into your operating systems: **TPRM/GRC, procurement, ticketing**



90 day plan

A realistic roadmap to move from periodic to continuous

Weeks 1–2

- Tier vendors by criticality
- Define minimum controls by tier
- Name owners and escalation paths

Weeks 3–6

- Automate evidence intake and control mapping for top-tier vendors
- Standardize gap handling and exceptions

Weeks 7–10

- Enable continuous monitoring for top-tier vendors
- Set thresholds that map to actions

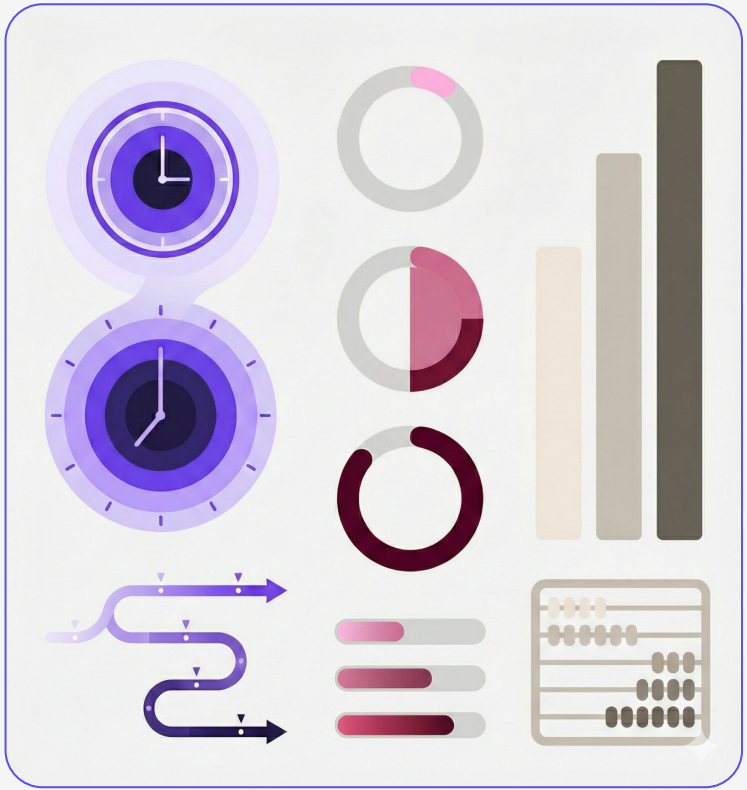
Weeks 11–13

- Implement trigger-based workflows, remediation SLAs, and reporting
- Measure cycle time from alert to proof of remediation

Metrics that matter

If you can’t measure it, you can’t defend it.

- Time to identify material third-party exposure
- Time to route to owner
- Time to remediation proof (median and P90)
- Percentage of critical vendors under continuous TPRM
- Number of risk acceptances with expiration dates
- Concentration risk visibility (critical services with single points of failure)



Wrap-up

If your third-party program is only compliant at renewal time, it's paperwork.

Continuous TPRM is the path to both compliance and real risk reduction.

- Continuous TPRM = "sensing + acting"
- Tier vendors, tune signals, operationalize remediation
- Use AI to remove low-signal work, not replace judgment
- Build audit readiness as an output, not the objective

SecurityScorecard

ODYSSEY 2026 CONF

Thank you!