Machine Learning Driven Third Party Risk Management at Scale

Head of Third Party Risk (TPRM) Oversight at Blockchain Based Company

CONF42 MACHINE LEARNING 2026

Speaker Introduction

Sagar Sudhir Behere

Head of Third Party Risk (TPRM) Oversight

Blockchain Based Company

Specializing in machine learning applications for enterprise risk management, third party risk oversight, and regulatory compliance in digital financial ecosystems.

The Modern TPRM Challenge

Enterprises now depend on hundreds or thousands of external vendors, creating complex attack surfaces with rapidly shifting risk signals. Traditional approaches periodic assessments, static questionnaires, manual reviews cannot keep pace with the velocity and scale of modern supply chains.

Heightened regulatory expectations demand transparency, explainability, and continuous oversight that legacy systems simply cannot deliver.

Traditional TPRM: Structural Misalignment

Calendar-Based Reviews

Annual or quarterly assessments miss real-time risk changes and emerging threats between review cycles.

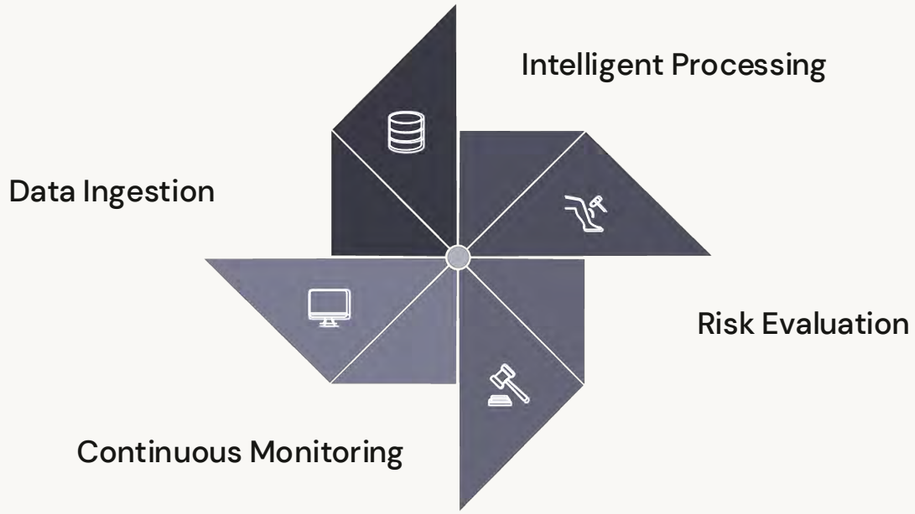
Static Questionnaires

One-size-fits-all surveys generate redundant questions and fail to adapt to vendor-specific risk profiles.

Manual Evidence Review

Human-driven analysis of unstructured documents creates bottlenecks, inconsistency, and scaling limitations.

The ML Transformation: Core Architecture



Machine learning transforms TPRM into an intelligence-driven capability through automated evidence extraction, dynamic assessment tailoring, multi-model verification, and event-driven monitoring.

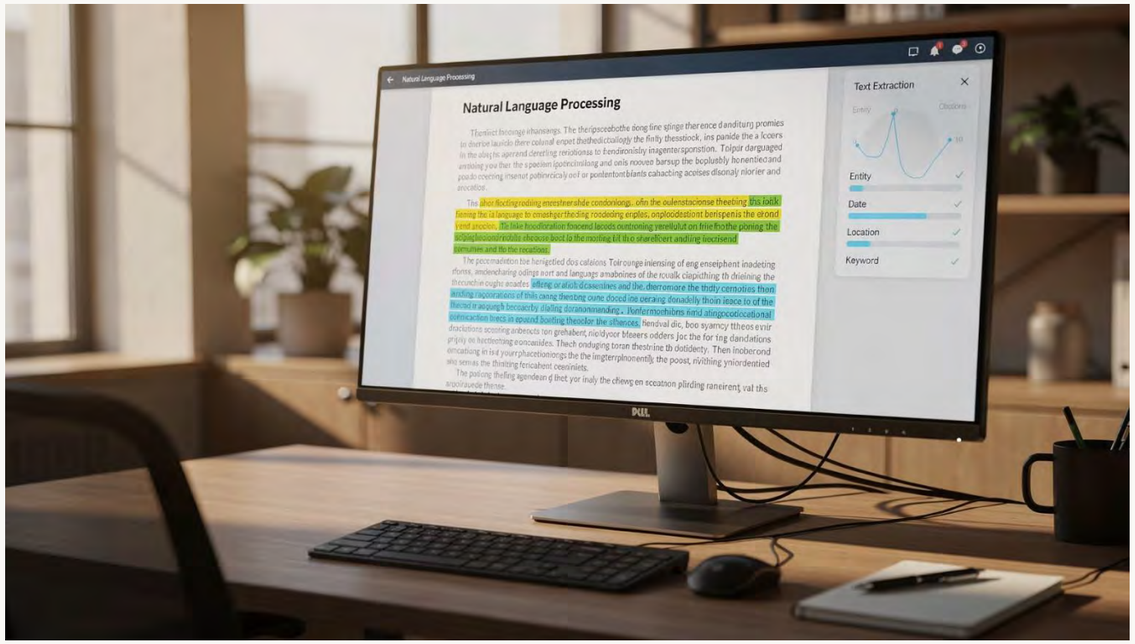
This architecture operates continuously rather than episodically, adapting to each vendor's unique risk surface.

NLP for Evidence Extraction

Automating Control Evidence Analysis

Natural language processing models extract and normalize control evidence from unstructured vendor artifacts security policies, audit reports, certifications, and compliance documentation.

This automation reduces manual workload by processing thousands of documents while maintaining complete traceability for audit purposes.



Semantic Similarity & Intelligent Clustering

Eliminate Redundancy

Clustering techniques identify duplicate or overlapping questions across assessment frameworks, streamlining vendor burden.

Dynamic Tailoring

Semantic similarity algorithms customize follow-up questions based on vendor responses and risk profile, creating adaptive workflows.

Context-Aware Routing

Models route specialized questions to appropriate vendor stakeholders, improving response quality and efficiency.

Ensemble Modeling & Multi-Model Verification

Cross-Validation at Scale

Our approach leverages multiple independent models to rigorously cross-validate risk data. This mitigates single-model bias and proactively identifies critical discrepancies. Each risk determination is equipped with confidence scores, automatically flagging low-confidence cases for expert human review essential for robust governance and regulatory explainability.

Continuous Monitoring Architecture

From Periodic Reviews to Event-Driven Detection

Leveraging ML, our continuous monitoring replaces periodic reviews with real-time risk detection. We ingest diverse data streams from threat intelligence and security advisories to financial indicators and behavioral anomalies automatically triggering reassessments when material risk changes are identified.

Data Sources for Continuous Intelligence

Threat Intelligence

Real-time cyber threat feeds and vulnerability databases

Security Advisories

CVE disclosures and vendor security bulletins

Financial Indicators

Credit ratings, earnings reports, and market signals

Public Disclosures

Breach notifications and regulatory filings

Behavioral Patterns

Anomalous vendor activity and operational changes

Predictive Risk Detection

Early-Warning Pattern Recognition

Predictive algorithms trained on historical incident data identify early-warning patterns across critical domains: cybersecurity vulnerabilities, operational resilience degradation, and financial stability concerns.

These models detect subtle signals that precede material risk events, enabling proactive intervention before incidents occur.

Explainability & Regulatory Compliance

1

Transparent Reasoning

Models provide human-interpretable explanations for risk scores, showing which factors drove each conclusion.

2

Audit Trail Preservation

Complete traceability from source data through model decisions to final risk determinations.

3

Regulatory Alignment

Architecture designed to meet transparency requirements from financial regulators and compliance frameworks.

Business Impact & Outcomes

Operational Scale

Assess and monitor thousands of vendors continuously without proportional headcount growth

Response Velocity

Detect and respond to emerging risks in hours rather than weeks or months

Consistency

Standardized evaluation methodology reduces subjective variation in risk assessments

Strategic Intelligence

TPRM becomes a core capability providing actionable insights to executive leadership

Positioning TPRM as Core Intelligence

Machine learning elevates third-party risk management from a compliance checkbox to a strategic intelligence capability within resilient digital ecosystems.

By combining scalability, explainability, and adaptability, ML-driven TPRM enables enterprises to confidently navigate complex vendor dependencies while meeting rigorous regulatory expectations.

Thank You!

Sagar Sudhir Behere

Head of Third Party Risk (TPRM) Oversight

Conf42 Machine Learning 2026