

THIRD-PARTY
RISK MANAGEMENT.

The discipline of **vetting, tiering, contracting, and continuously monitoring** every vendor, supplier, and partner that touches your data or systems. A signed contract proves obligation — it never proves compliance.

VENDOR DUE DILIGENCE

SOC 2 / ISO 27001

FOURTH-PARTY RISK

CONTINUOUS MONITORING

01 THE MECHANISM

Vendor Inventory & Tiering
Every third party is catalogued and risk-tiered by data access, system criticality, and business impact before any assessment begins.

Due Diligence & Assessment
Scoped to tier, **questionnaires, SOC 2 reports, and financial checks** validate posture before a contract is ever signed.

Continuous Monitoring
After onboarding, **ratings services, breach feeds, and SLA tracking** catch posture drift long before the next scheduled review.

02 THE FLOW

The Onboarding Cycle PRE-CONTRACT

1

Vendor is identified and **risk-tiered** based on data access and business criticality.

2

A **due diligence assessment** — questionnaire, SOC 2, financial review — is scoped to that tier.

3

Contract is signed with **security requirements, SLAs, and right-to-audit** clauses attached.

The Monitoring Cycle POST-CONTRACT

1

A **reassessment cadence** is set by tier — annual for critical, biennial for lower risk.

2

Continuous monitoring feeds — ratings, breach alerts, financial signals — are reviewed in real time.

3

Issues trigger a **remediation plan, escalation, or offboarding decision**.

03 VENDOR TIERS & ASSESSMENT DEPTH

TIER	ASSESSMENT REQUIREMENT
Tier 1 — Critical	Full audit (onsite or virtual); SOC 2 Type II required; annual reassessment.
Tier 2 — High	Security questionnaire plus SOC 2 Type I or equivalent; annual reassessment.
Tier 3 — Moderate	Lightweight questionnaire; biennial reassessment.
Tier 4 — Low	Self-attestation only; reassessed at contract renewal.

04 VENDOR RISK SIGNALS COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
Security Questionnaire	No	Self-reported; no independent verification of the answers.
SOC 2 Report	No	A point-in-time snapshot that may not cover subcontractors or new products.
Security Rating Service	No	External scan of internet-facing posture only; misses internal controls.
Contractual Clauses	No	Defines the obligation, but doesn't confirm the vendor is actually meeting it.
Combined TPRM Program (Tiering + Assessment + Monitoring + Contract)	Yes	Ties classification, verification, and ongoing oversight into one accountable framework.

THIRD-PARTY RISK.

TIER · ASSESS · MONITOR

05 PROGRAM OPERATIONS

Risk tiering drives everything downstream. Assess proportional to risk — a critical processor and a low-risk supplier don't get the same scrutiny.

Fourth-party risk is real. Your vendor's own vendors and subcontractors carry risk you inherit but rarely see.

Offboarding is a control, not an afterthought. Access must be revoked, data returned or destroyed, and contracts closed cleanly.

Concentration risk matters. Too many critical functions resting on one vendor creates a single point of failure.

06 CONTROL MAPPING

NIST SP 800-161

Supply chain risk management practices for organizations and information systems.

ISO/IEC 27036

Guidance for **information security in supplier relationships** across the vendor lifecycle.

SIG / SIG LITE

Standardized Information Gathering questionnaires used across the industry for **vendor assessments**.

OCC / FFIEC GUIDANCE

Regulatory expectations for **third-party risk oversight** at financial institutions.

07 WHAT TPRM DOES NOT SOLVE

Fourth-party & subcontractor risk

Visibility typically stops at the **direct vendor relationship**, not who they in turn rely on.

Shadow IT & unapproved vendors

Tools procured **outside the vetting process** never enter the program at all.

Unenforced contractual promises

SLAs and security clauses that go **unmonitored** become worthless the moment they're signed.

Vendor concentration risk

A single critical vendor's outage or breach can **cascade across multiple business functions** at once.

08 MYTHS VS. REALITY

MYTH "A SOC 2 report means the vendor is secure."	REALITY It's a point-in-time snapshot scoped to specific controls — it doesn't cover new products, regions, or subcontractors.
MYTH "Once a vendor passes assessment, we're done."	REALITY Risk posture changes constantly — continuous monitoring , not a one-time gate, is what keeps the picture current.
MYTH "Only vendors with data access need review."	REALITY Operational and availability dependencies — like critical SaaS uptime — carry real risk with no data ever changing hands.
MYTH "Contract language equals control."	REALITY Contracts define the obligation ; they never verify the vendor is actually meeting it in practice.
MYTH "TPRM is procurement's job."	REALITY Security, legal, and the business owner share accountability across the entire vendor lifecycle.

09 SPEAK THE PROGRAM — KEY TERMS

FOURTH-PARTY RISK

Risk introduced by your **vendor's own vendors** or subcontractors, one step removed from direct oversight.

SIG QUESTIONNAIRE

Standardized Information Gathering — an **industry-standard vendor assessment** questionnaire from Shared Assessments.

SOC 2 TYPE I VS II

Type I reviews control **design at a point in time**; Type II tests **operating effectiveness over a period**.

VENDOR TIERING

Classifying vendors by **criticality and data access** so assessment depth matches actual risk.

RIGHT TO AUDIT

A contract clause granting the organization the ability to **verify vendor controls directly**.

CONCENTRATION RISK

Exposure created when **too many critical functions** depend on a single vendor.