

TPRM Program Maturity Assessment Rubric

Nine-Dimension, Five-Level Scoring Framework

Available at www.tpvrm.net/documents | *The Future of Third-Party Risk Management & Data Privacy*

This rubric offers a structured framework for assessing the current maturity of a Third-Party Risk Management (TPRM) program. Organizations should perform a maturity assessment before creating or updating an implementation roadmap, and should conduct the assessment at least once a year to monitor progress. The rubric evaluates nine dimensions on a five-level scale. Fractional scores (e.g., 2.5) can be used when a program exhibits characteristics of two neighboring levels.

LEVEL DEFINITIONS

Level 1: Initial	TPRM activities are ad hoc, informal, and reactive. No documented policies or standards exist. Risk management depends on individual knowledge rather than institutional process. Vendor inventory may not exist.
Level 2: Foundational	Basic TPRM policies are documented and approved. A vendor inventory exists but may be incomplete. Risk assessments are conducted at onboarding but not revisited. Standard questionnaire templates are in use with inconsistent follow-up. Some contractual protections are in place.
Level 3: Defined	TPRM is a documented, consistently applied program. Complete vendor inventory with risk tiering. Risk assessments at onboarding and on a defined periodic schedule. Standard questionnaire and evidence review. Required contract provisions applied consistently. Defined escalation and issue management process.
Level 4: Managed	TPRM is metrics-driven and continuously monitored. AI governance and privacy criteria integrated into assessments. Continuous monitoring for Tier 1 vendors. Executive and board-level reporting. Risk-based prioritization. Technology platforms support process efficiency. Program performance is measurable and tracked over time.
Level 5: Optimized	TPRM is a strategic enterprise capability. AI-assisted risk assessment and anomaly detection. Predictive risk identification. Program continuously adapts to emerging threats and regulatory changes. TPRM outcomes directly inform business strategy and vendor selection. Cross-functional integration with legal, privacy, procurement, and business lines is seamless.

NINE-DIMENSION RUBRIC

For each dimension, choose the level that best represents the program's current state. Use fractional scores (e.g., 2.5) when the program clearly surpasses one level but does not fully meet the next.

DIMENSION 1: Program Governance

Dimension	Level 1 Initial	Level 2 Foundational	Level 3 Defined	Level 4 Managed	Level 5 Optimized
Program Governance	No TPRM policy exists. Risk management is	Basic TPRM policy exists but may not be	TPRM policy formally approved. Board	TPRM integrated into enterprise risk	TPRM informs business strategy. AI-

Dimension	Level 1 Initial	Level 2 Foundational	Level 3 Defined	Level 4 Managed	Level 5 Optimized
	informal and reactive.	current. Limited leadership awareness.	and senior management awareness. Defined program charter.	framework. Regular senior/board reporting. Formal TPRM committee.	driven governance insights. Continuous regulatory alignment.
ASSIGNED SCORE	[] 1.0	[] 2.0	[] 3.0	[] 4.0	[] 5.0

DIMENSION 2: Vendor Inventory and Tiering

Dimension	Level 1 Initial	Level 2 Foundational	Level 3 Defined	Level 4 Managed	Level 5 Optimized
Vendor Inventory & Tiering	No comprehensive vendor inventory. Vendor relationships undocumented or fragmented.	Partial vendor inventory exists. Informal tiering or no tiering applied.	Complete vendor inventory maintained. Formal risk tiering methodology applied consistently.	Automated inventory management. Tiering reviewed annually or on material change. Fourth-party visibility for Tier 1.	Dynamic, real-time inventory. AI-assisted tiering updates. Full supply chain visibility including Nth-party risk.
ASSIGNED SCORE	[] 1.0	[] 2.0	[] 3.0	[] 4.0	[] 5.0

DIMENSION 3: Due Diligence and Assessment

Dimension	Level 1 Initial	Level 2 Foundational	Level 3 Defined	Level 4 Managed	Level 5 Optimized
Due Diligence & Assessment	No formal assessment process. Assessments conducted ad hoc if at all.	Standard questionnaire used but inconsistently. Evidence review rare. No periodic reassessment.	Tiered assessment framework applied at onboarding and on periodic schedule. Evidence review for Tier 1. AI-specific questions for applicable vendors.	Risk-based assessment depth. Continuous monitoring supplements periodic assessment. AI and privacy criteria integrated.	Predictive assessment triggers. AI-assisted evidence analysis. Assessment correlated with threat intelligence.
ASSIGNED SCORE	[] 1.0	[] 2.0	[] 3.0	[] 4.0	[] 5.0

DIMENSION 4: Contracting

Dimension	Level 1 Initial	Level 2 Foundational	Level 3 Defined	Level 4 Managed	Level 5 Optimized
Contracting	No standard contract provisions. Security and	Some security provisions in most contracts. DPAs	Standard contract templates with required	AI-specific clauses and ESG provisions for applicable	Contract provisions dynamically updated to

Dimension	Level 1 Initial	Level 2 Foundational	Level 3 Defined	Level 4 Managed	Level 5 Optimized
	privacy obligations absent or inconsistent.	inconsistently applied.	security, privacy, and AI provisions. Legal reviews all Tier 1 and Tier 2 contracts.	vendors. Subprocessor flow-down consistently implemented.	reflect regulatory changes. Automated contract review tools identify gaps.
ASSIGNED SCORE	[] 1.0	[] 2.0	[] 3.0	[] 4.0	[] 5.0

DIMENSION 5: Continuous Monitoring

Dimension	Level 1 Initial	Level 2 Foundational	Level 3 Defined	Level 4 Managed	Level 5 Optimized
Continuous Monitoring	No ongoing monitoring. Awareness of vendor issues depends on vendor-initiated notification.	Ad hoc monitoring when issues surface. Financial health reviewed inconsistently.	Defined monitoring cadence by tier. Financial, operational, reputational, and compliance triggers tracked. Incident notification processes in place.	Automated monitoring tools for Tier 1. External threat intelligence integrated. Material change triggers reassessment.	Real-time monitoring with AI-assisted anomaly detection. Predictive risk signals. Fourth-party continuous monitoring.
ASSIGNED SCORE	[] 1.0	[] 2.0	[] 3.0	[] 4.0	[] 5.0

DIMENSION 6: Issue Management and Remediation

Dimension	Level 1 Initial	Level 2 Foundational	Level 3 Defined	Level 4 Managed	Level 5 Optimized
Issue Management & Remediation	No formal issue tracking. Finding resolution is ad hoc and untracked.	Issues documented informally. No defined SLAs. Escalation path unclear.	Structured issue tracking with defined SLAs by severity. Clear escalation path. Remediation evidence required for closure.	Remediation performance tracked and reported. Risk acceptance documented and time-limited. Systemic issues identified across vendor portfolio.	Predictive identification of emerging issues. AI-assisted remediation prioritization. Portfolio-level risk pattern detection.
ASSIGNED SCORE	[] 1.0	[] 2.0	[] 3.0	[] 4.0	[] 5.0

DIMENSION 7: Reporting and Metrics

Dimension	Level 1 Initial	Level 2 Foundational	Level 3 Defined	Level 4 Managed	Level 5 Optimized
Reporting & Metrics	No TPRM metrics or reporting. Program	Basic activity metrics (assessments completed,	Defined KPI and KRI set. Regular reporting to TPRM	Board-level TPRM reporting. Metrics tied to business	AI-driven metric insights. Predictive KRIs. TPRM metrics

Dimension	Level 1 Initial	Level 2 Foundational	Level 3 Defined	Level 4 Managed	Level 5 Optimized
	performance invisible to leadership.	vendors inventoried). Inconsistent reporting.	leadership and senior management. Tier 1 dashboard maintained.	outcomes. Trend analysis and benchmarking.	integrated into enterprise risk reporting frameworks.
ASSIGNED SCORE	[] 1.0	[] 2.0	[] 3.0	[] 4.0	[] 5.0

DIMENSION 8: Organizational Capability

Dimension	Level 1 Initial	Level 2 Foundational	Level 3 Defined	Level 4 Managed	Level 5 Optimized
Organizational Capability	No designated TPRM role. Responsibility fragmented or implicit.	Designated TPRM role exists. Limited staffing. Training informal.	Defined TPRM function with documented RACI. Regular training for TPRM staff and business unit stakeholders.	AI risk and privacy expertise embedded in TPRM. Cross-functional integration with legal, privacy, IT, and procurement.	TPRM competency model defined. Industry engagement. Continuous learning program. TPRM capability shared with supply chain partners.
ASSIGNED SCORE	[] 1.0	[] 2.0	[] 3.0	[] 4.0	[] 5.0

DIMENSION 9: Technology and Tools

Dimension	Level 1 Initial	Level 2 Foundational	Level 3 Defined	Level 4 Managed	Level 5 Optimized
Technology & Tools	TPRM managed manually in spreadsheets or email. No dedicated tooling.	Basic GRC or vendor management tools used for some functions. Limited integration.	Dedicated TPRM platform (GRC, VRMS, or equivalent). Questionnaire distribution and tracking automated. Assessment records centralized.	Platform integrates with continuous monitoring data feeds, contract management, and issue tracking. Dashboards for all tiers.	AI-assisted assessment and risk scoring. Automated regulatory mapping. API integration with enterprise systems. Predictive analytics.
ASSIGNED SCORE	[] 1.0	[] 2.0	[] 3.0	[] 4.0	[] 5.0

SCORING SUMMARY

Complete the scoring summary after assessing all nine dimensions. The Overall Maturity Score is a weighted average. Adjust weights based on your regulatory environment and risk priorities. Default equal weighting assigns 11.1% per dimension.

Dimension	Assigned Score (1-5)	Weight (%)	Weighted Score	Priority Gap
Program Governance		11.1%		☐ H ☐ M ☐ L
Vendor Inventory & Tiering		11.1%		☐ H ☐ M ☐ L
Due Diligence & Assessment		11.1%		☐ H ☐ M ☐ L
Contracting		11.1%		☐ H ☐ M ☐ L
Continuous Monitoring		11.1%		☐ H ☐ M ☐ L
Issue Management & Remediation		11.1%		☐ H ☐ M ☐ L
Reporting & Metrics		11.1%		☐ H ☐ M ☐ L
Organizational Capability		11.1%		☐ H ☐ M ☐ L
Technology & Tools		11.1%		☐ H ☐ M ☐ L
OVERALL MATURITY SCORE		100%		

Score Interpretation

Score Range	Interpretation and Priority Action
1.0 - 1.9	High Risk. Immediate action required. Focus on establishing basic policy, vendor inventory, and intake process. Regulatory exposure is elevated.
2.0 - 2.9	Elevated Risk. Focus on formalizing processes, completing vendor inventory, and establishing consistent assessment and contracting practices. Phase 1 roadmap applies.
3.0 - 3.9	Moderate Risk. Program is functioning but needs enhancement in monitoring, metrics, and AI/privacy integration. Phase 2 roadmap applies.
4.0 - 4.9	Low-Moderate Risk. Program is well-managed. Focus on optimization, predictive capabilities, and enterprise integration. Phase 3 roadmap applies.
5.0	Low Risk. Optimized program. Maintain through continuous improvement and adapt to emerging threats and regulatory changes.

Assessment Conducted By	
Assessment Date	
Next Assessment Due	