# TPRM RACI MATRIX TEMPLATE

Roles and Responsibilities Across the Vendor Lifecycle

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

This RACI matrix outlines roles and responsibilities for each activity in the TPRM vendor lifecycle. Customize role names to match your organization's structure. Each activity must have exactly one "A" (Accountable) and at least one "R" (Responsible). "C" (Consulted) roles offer input before completion. "I" (Informed) roles are notified of outcomes.

## RACI LEGEND

| | | | |
|---|---|---|---|
| **R** | Responsible: Does the work to complete the task. Multiple R roles may apply. | **A** | Accountable: Owns the outcome. Exactly one A per activity. |
| **C** | Consulted: Provides input before the task is completed. Two-way communication. | **I** | Informed: Notified of outcomes. One-way communication. |

## TPRM RACI MATRIX

Column headers represent organizational functions. Adapt them to match your organization's structure. "TPRM" = TPRM function/team. "IT/Security" = IT Security or Information Security function.

| Phase | TPRM Activity | TPRM | Legal | Privacy | IT / Security | Procurement | Business Unit | Exec / Risk Committee |
|---|---|---|---|---|---|---|---|---|
| **Intake** | Vendor request received and logged | R | I | I | I | C | R | I |
| **Intake** | ITC completion coordinated with business unit | R | C | C | C | I | R | I |
| **Intake** | ITC reviewed and scope assessment validated | **A** | - | - | C | - | C | I |
| **Intake** | Risk tier assigned based on ITC outcome | **A** | C | C | C | I | I | I |
| **Intake** | DPIA/PIA triggered and initiated (if applicable) | C | C | **A** | - | I | I | I |
| **Assessment** | Questionnaire selected and distributed to vendor | **A** | - | C | C | I | I | I |
| **Assessment** | Vendor questionnaire response reviewed | R | - | C | C | - | - | I |
| **Assessment** | Evidence review (SOC 2, pen test, certifications) | R | - | C | R | - | - | I |
| **Assessment** | AI governance assessment (if applicable) | R | C | C | R | - | C | I |
| **Assessment** | Assessment findings documented and risk-rated | **A** | - | C | C | - | I | I |

| Phase | TPRM Activity | TPRM | Legal | Privacy | IT / Security | Procurement | Business Unit | Exec / Risk Committee |
|---|---|---|---|---|---|---|---|---|
| **Assessment** | Assessment outcome escalated to senior management (if needed) | R | C | C | C | I | C | A |
| **Contracting** | Contract review against ISA checklist | R | R | C | C | C | I | I |
| **Contracting** | DPA review and negotiation (if applicable) | C | R | A | - | - | I | I |
| **Contracting** | AI governance provisions negotiation (if applicable) | C | R | A | C | - | I | I |
| **Contracting** | Contract gap risk acceptance decision | C | C | C | C | C | I | A |
| **Contracting** | Final contract execution | I | A | I | I | R | C | I |
| **Onboarding** | Onboarding documentation and baseline established | R | C | C | R | I | R | I |
| **Onboarding** | Vendor added to TPRM risk register and inventory | A | - | I | I | I | I | I |
| **Onboarding** | Access provisioned per contractual requirements | C | I | C | A | I | R | I |
| **Onboarding** | Business unit vendor risk owner designated | C | I | I | I | I | A | I |
| **Monitoring** | Periodic reassessment scheduled and executed | A | - | C | C | - | I | I |
| **Monitoring** | Continuous monitoring alerts reviewed (Tier 1) | R | I | C | R | - | I | I |
| **Monitoring** | Material vendor change reviewed and assessed | A | C | C | C | C | R | I |
| **Monitoring** | Financial health / concentration risk review | A | C | - | - | C | C | I |
| **Monitoring** | Fourth-party / subprocessor review (Tier 1) | A | C | C | C | - | I | I |
| **Issues** | Vendor assessment finding documented | R | - | C | C | - | I | I |
| **Issues** | Remediation plan negotiated with vendor | A | C | C | C | - | I | I |
| **Issues** | Remediation evidence reviewed and finding closed | A | - | C | C | - | I | I |
| **Issues** | Risk acceptance documented for unresolved findings | C | C | C | C | - | C | A |
| **Issues** | Vendor incident notification received and triaged | R | R | R | R | I | R | A |
| **Offboarding** | Offboarding initiated and documented | A | C | C | C | R | R | I |
| **Offboarding** | Data return / destruction confirmed | C | C | A | R | - | I | I |
| **Offboarding** | Access revoked and | C | I | I | A | I | R | I |

| Phase | TPRM Activity | TPRM | Legal | Privacy | IT / Security | Procurement | Business Unit | Exec / Risk Committee |
|---|---|---|---|---|---|---|---|---|
| | systems disconnected | | | | | | | |
| **Offboarding** | Vendor record archived in TPRM system | **A** | I | I | I | I | I | I |
| **Reporting** | TPRM metrics compiled and reported to management | **A** | I | I | C | I | I | I |
| **Reporting** | Board / executive TPRM reporting | R | C | C | C | I | I | **A** |
| **Reporting** | Annual program review and maturity assessment | **A** | C | C | C | C | C | I |

## CUSTOMIZATION GUIDE

Step 1: Substitute the generic role titles (Legal, Privacy, IT/Security, Procurement, Business Unit, Exec/Risk Committee) with your organization's specific role titles and team names.

Step 2: Review each activity and adjust RACI designations to match your organizational structure. In smaller organizations, one team may assume multiple roles. In larger organizations, activities might be further subdivided.

Step 3: Confirm with stakeholders. Each function should review the activities they are responsible for or accountable to and verify they have the authority, resources, and access needed to fulfill that role.

Step 4: Make sure each activity has exactly one "A." If you find activities with no or multiple "A" labels, fix those before completing the process.

Step 5: Record the approved RACI in your TPRM program policy and ensure it is accessible to all participating functions. Review and update it annually or whenever there are significant organizational changes.

| | |
|---|---|
| **RACI Approved By** | |
| **Approval Date** | |
| **Next Review** | |