**Third-Party Continuous Monitoring Program Simulation**

**Objective**

To design a lightweight, scalable program for ongoing monitoring of third-party risk post-onboarding — focusing on risk indicators, automation triggers, periodic reassessment, and escalation thresholds.

**KRI-to-Risk Tier Mapping Table**

This shows which Key Risk Indicators (KRIs) should apply to each Risk Tier (High, Medium, Low). This ensures the ongoing monitoring is proportional to vendor risk and aligns with best practices.

**Criticality Tiers Explained**

| **Criticality** | **What It Means** | **Examples** |
| --- | --- | --- |
| **Critical** | Business cannot operate without the vendor; disruption = high risk or downtime | Cloud provider, identity platform |
| **High** | Significant operational or compliance impact; may handle sensitive/confidential data | Payroll processor, claims platform |
| **Medium** | Important but not mission-critical; may affect team workflows or data indirectly | Document e-sign, analytics tools |
| **Low** | Limited impact; often replaceable; doesn’t handle sensitive data | Marketing, hardware vendors |

**KRI Explanations – Function and Logic**

| **KRI** | **What It Measures** | **How It Works** | **Trigger / Threshold** | **Why It Matters** |
| --- | --- | --- | --- | --- |
| Outstanding Risk Remediation | Tracks open residual risks with accepted remediation timelines from the onboarding phase or periodic reassessments. Triggers when remediation deadlines are missed or repeatedly extended without justification. | Track open findings (from risk assessments, audits, or questionnaires) and flag if not remediated within a set number of days | > 60 days without closure or mitigation plan | Indicates that the vendor may not be prioritizing risk management or compliance |
| Policy/Cert Expiry | Tracks if vendor’s key certifications (e.g., SOC 2, ISO 27001) or security policies are current | Log the expiration dates of certs/docs; alert 30–45 days before expiry | Expiring within 30 days or already expired | Expired or missing certifications = stale security posture and increased regulatory risk |
| SLA/Uptime Breach | Detects violations in service-level agreements (availability, uptime, response times) | Pull reports or auto-monitor uptime against agreed SLAs (e.g., 99.9%) | >1 SLA breach in a quarter | Poor reliability signals operational risk, possible service disruption |
| Negative OSINT / Breach Alert | Flags publicly available negative news about the vendor (e.g., breach, regulatory fine, data leak) | Monitor threat intel, news feeds, or security advisories for vendor mentions | Any confirmed adverse cyber event or legal action | Uncovers reputational or security risk not reported directly by the vendor |
| Overdue Questionnaire / Risk Response | Monitors vendor responsiveness to periodic reassessments or follow-ups | Track due dates of annual risk questionnaires or issue responses | > 2 unanswered requests or 30+ days overdue | Lack of responsiveness may signal disengagement, immaturity, or risk evasion |
| Personnel Offboarding Lag | Checks whether vendors are promptly revoking access for offboarded personnel. Ask this in the annual or periodic vendor risk questionnaire. If the vendor fails to comply (e.g., access still active after separation), log that as a KRI trigger | Compare termination dates to actual access revocation dates (manual or system-fed) | >5 business days between termination and access removal | Delayed access removal is a direct control failure, exposing your systems/data |
| Change in Service / Subcontractors | Detects major shifts in vendor environment (ownership, hosting, 4th-party use) | Log self-reported changes, procurement updates, or service change notices | Any material change in systems, 3rd/4th parties, or data flows | Changes may invalidate prior risk assessments or bypass contractual controls |
| Unreviewed Contract > 24 Months | Tracks whether vendor contracts have had any recent security/legal review | Timestamp last review; trigger if over 24 months old | >24months since last security/legal review | Prevents stale clauses, missing regulatory updates, or outdated risk allocations |

**Monitoring Workflow**

New KRI Trigger → Check against Thresholds → Log in Risk Register → Notify Stakeholders → Require Vendor Action → Escalate if Unresolved