Introduction to Third-Party Risk Management (TPRM)

Third-Party Risk Management (TPRM) is the structured approach to identify, assess, monitor, and govern risks introduced by external parties across their entire lifecycle.

Enhanced Feature Architecture

1. Core Modules (Application Layer)

These modules manage the complete lifecycle of third-party risk — from onboarding to continuous assurance.

1.1 Vendor Governance & Onboarding

Purpose: Establish structured vendor identity, ownership, and contractual accountability.

Features:

- Vendor profile management (legal entity, ownership, jurisdiction, criticality tier)
- Vendor classification (Critical, High, Medium, Low risk tiers)
- Contract lifecycle management (contracts, NDAs, DPAs, SLAs)
- Vendor ownership assignment (Business owner, Risk owner, Contract owner)
- Vendor segmentation by service type (IT, Cloud, Supplier, Consultant, Partner)
- Vendor portal access provisioning
- Vendor offboarding and termination workflow

Improvement Added: Vendor criticality tiering and ownership accountability (essential for regulators like SAMA, NCA).

1.2 Third-Party Risk Assessment Module

Purpose: Identify and quantify inherent and residual risk.

Features:

- Configurable risk questionnaires (Cyber, Privacy, ESG, Operational, Financial)
- Framework-based assessments (ISO 27001, NCA, SAMA, NIST, GDPR)
- Automated risk scoring engine (inherent and residual risk)
- Conditional questionnaires based on vendor type and criticality
- Control effectiveness evaluation
- Vendor self-assessment and internal assessment modes
- Assessment version history and audit trail

Improvement Added: Conditional assessments and inherent vs residual risk separation.

1.3 Third-Party Risk Register

Purpose: Centralized repository of all vendor risks.

Features:

- Vendor-linked risk register
- Risk categorization (Cyber, Operational, Financial, Compliance, ESG)
- Risk scoring (Likelihood, Impact, Residual risk)
- Risk ownership assignment
- Risk treatment plans and remediation tracking
- Risk acceptance, transfer, mitigation, avoidance workflows
- Risk history and audit trail

Improvement Added: Full risk lifecycle management (not just score storage).

1.4 Compliance & Regulatory Mapping Module

Purpose: Ensure vendor compliance with regulatory and contractual obligations.

Features:

- Mapping vendor controls to frameworks:
  - SAMA
  - NCA ECC
  - ISO 27001
  - GDPR
  - NIST CSF
  - Internal policies
- Compliance gap identification
- Automated compliance scoring
- Vendor compliance posture tracking
- Evidence-based compliance validation

Improvement Added: Multi-framework mapping and compliance scoring.

1.5 Continuous Monitoring Module

Purpose: Move from periodic assessment to continuous risk visibility.

Features:

- SLA monitoring and breach detection
- Contract expiry and renewal alerts
- Certification expiry tracking (ISO, SOC2, etc.)
- Vendor performance tracking

- Continuous risk score recalculation
- Vendor status tracking (Active, Suspended, Terminated)
- Risk threshold breach alerts

Improvement Added: Continuous risk score recalculation.

1.6 Incident & Issue Management Module

Purpose: Capture and manage vendor-related incidents.

Features:

- Third-party incident reporting
- SLA violation tracking
- Breach and security incident logging
- Root cause analysis tracking
- Remediation and containment workflows
- Incident-to-risk linkage
- Incident impact scoring

Improvement Added: Full incident lifecycle and risk linkage.

1.7 Third-Party Audit & Evidence Management

Purpose: Maintain defensible audit-grade assurance.

Features:

- Vendor evidence repository
- Evidence versioning and integrity protection
- Evidence expiry tracking
- Audit findings management
- Audit planning and execution
- Audit trail and immutable logs

Improvement Added: Evidence lifecycle management.

1.8 Executive Reporting & Risk Intelligence Dashboards

Purpose: Provide real-time executive visibility.

Features:

- Vendor risk heatmaps
- Critical vendor exposure dashboard
- Compliance posture dashboard
- Risk trend analysis
- Vendor risk ranking
- Executive summary dashboards
- Board-level reporting

Improvement Added: Executive and board-level intelligence views.

2. Automation Layer (DIFLOW – DiGRC Workflow Engine)

Purpose: Automate the entire TPRM lifecycle.

Core Automation Capabilities

- Automated vendor onboarding workflows
- Automated assessment scheduling
- SLA breach workflow automation
- Risk escalation workflows
- Automated reassessment scheduling
- Automated contract renewal workflows
- Auto-assignment of risk owners
- Auto-remediation workflow initiation
- Approval workflows (Legal, Risk, Compliance)
- Vendor offboarding workflows

Key Differentiator: Low-code automation engine fully integrated with risk lifecycle.

3. AI Intelligence Layer (Gracie AI for TPRM)

This is your strongest differentiator.

3.1 AI Vendor Response Analysis

- Detect contradictory vendor responses
- Identify incomplete or suspicious responses
- Flag risk indicators automatically

3.2 AI Risk Benchmarking Engine

- Compare vendor risk posture with industry peers
- Benchmark vendors by:

- Industry
- Geography
- Vendor type

3.3 AI Predictive Risk Intelligence

- Detect early risk signals from:
  - Sanctions lists
  - Cyber breach feeds
  - Financial distress indicators
  - Regulatory enforcement actions

3.4 AI Continuous Risk Monitoring

- Monitor vendor risk posture continuously
- Automatically update risk scores

3.5 AI Risk Remediation Recommendations

- Suggest remediation actions
- Suggest compensating controls
- Suggest mitigation strategies

3.6 AI Vendor Criticality Recommendation

- Suggest vendor risk tier automatically

4. Data Layer (Foundation Layer)

Centralized, structured, and secure.

Core Databases

4.1 Vendor Registry Database

- Vendor identity
- Ownership
- Classification

4.2 Risk Register Database

- Risk scores
- Risk history
- Risk treatment plans

4.3 Compliance Obligations Database

- Framework mappings
- Regulatory requirements

4.4 Evidence Repository

- Immutable audit records
- Certifications and documents

4.5 Incident Database

- Incident logs
- Impact tracking

5. Integration Layer

Critical for enterprise-grade TPRM.

5.1 External Intelligence Integrations

- Sanctions lists (OFAC, UN, EU)
- Cyber threat intelligence feeds
- Financial risk feeds
- Regulatory updates

5.2 Internal Enterprise Integrations

- ERP systems
- Procurement systems
- IAM systems
- Contract management systems

5.3 Vendor Portal

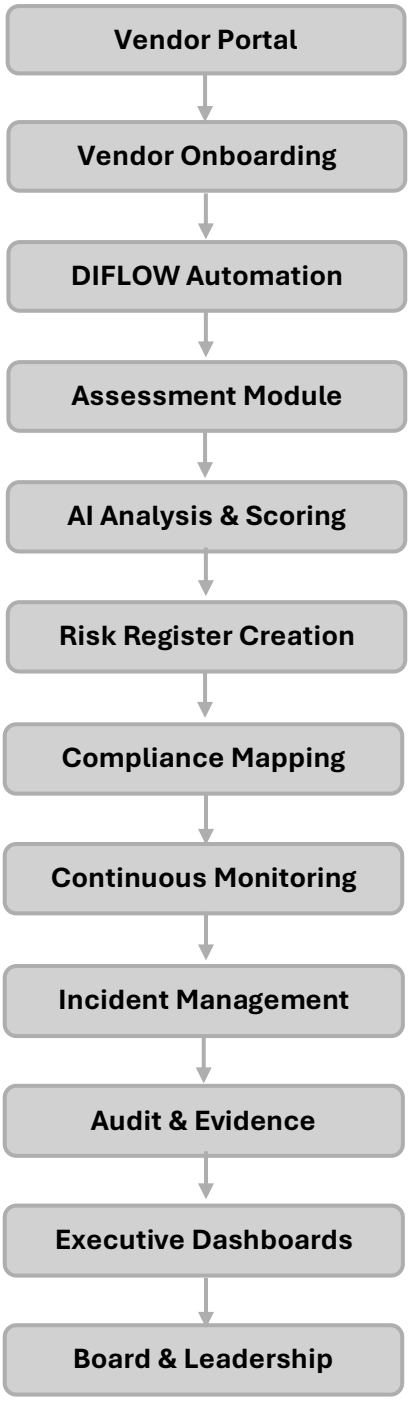
Secure portal where vendors can:

- Complete onboarding
- Submit assessments
- Upload certifications
- Submit evidence
- Track remediation tasks

6. Full Lifecycle Flow Architecture

This is extremely important for positioning.

Complete TPRM Lifecycle Flow



7. Strategic Positioning Statement (Recommended for Sales)

DiGRC TPRM transforms third-party risk management from periodic vendor assessments into a continuous, intelligence-driven risk assurance system — combining governance, automation, and AI-driven risk intelligence into a single unified platform.

8. Key World-Class Improvements Added

Area	Improvement
Vendor governance	Vendor ownership, tiering, lifecycle
Risk	Full lifecycle risk treatment
Compliance	Multi-framework mapping
Monitoring	Continuous risk recalculation
Incident	Full incident lifecycle
Audit	Evidence lifecycle management
Automation	Full workflow automation
AI	Predictive vendor risk intelligence
Executive	Board-level risk intelligence
Integration	External intelligence feeds