How to Mature a TPRM Program

KAIH TAYLOR
MANAGER THIRD-PARTY RISK MANAGEMENT

AGFIRST FARM CREDIT BANK

Maturity Assessments

HOW TO MOVE THE DIAL ON YOUR PROGRAM

Purpose of a Maturity Assessment

CURRENT STATUS EVALUATION

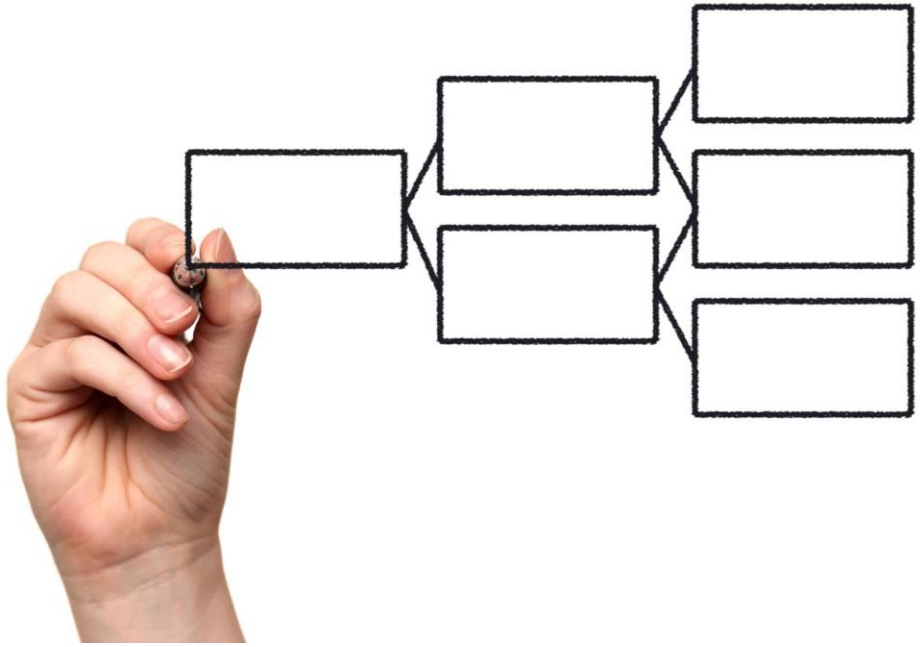
A maturity assessment helps determine the current status of your program, identifying strengths and weaknesses.

IDENTIFYING IMPROVEMENT AREAS

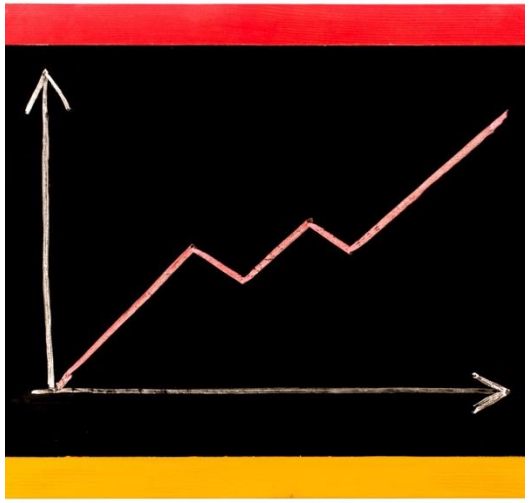
This assessment highlights areas requiring improvement to enhance overall program effectiveness and maturity.

ACHIEVING DESIRED MATURITY LEVELS

Understanding maturity levels guides programs toward achieving their desired outcomes and strategic goals.



Criteria for Evaluating Maturity Levels



Risk Identification

Effective maturity evaluation begins with thorough risk identification to understand potential vulnerabilities and threats.

Assessment Processes

Well-defined assessment processes ensure systematic evaluation of maturity levels, helping organizations identify gaps and areas for improvement.

Monitoring Practices

Ongoing monitoring practices are crucial for maintaining maturity levels and adapting strategies to changing environments.

Overall Governance

A strong governance framework supports maturity evaluations by establishing accountability and aligning objectives with organizational goals.

Tools and Methodologies for Assessment

Surveys for Assessment

Surveys are commonly used tools for gathering quantitative data about current practices and maturity levels in organizations.

Interviews as Methodology

Interviews provide qualitative insights and deeper understanding of current practices through direct interaction with stakeholders.

Scoring Models

Scoring models help quantify assessment results, allowing organizations to measure and compare maturity levels systematically.

Maturity Model

ADHOC

REACTIVE

PROACTIVE

Level 0 No Program	There is no/minimal management oversight of TPRM program
	Organization-level policies and procedures are either undocumented or nonexistent
Level 1 Initial	TPRM processes are ad hoc and review/re-review procedures are inconsistent
	Technology is not used for automating basic processes
Level 2 Defined	TPRM processes/workflows are existent but not implemented fully
	Interdependence among teams is not well established while executing TPRM tasks
Level 3 Managed	Standardized processes are applied consistently across full third-party risk lifecycle
	Risk metrics are well defined and enable enhanced decision-making. On demand reports
	Policies and standards are defined, documented and revised periodically
Level 4 Integrated	Utilize updated IRA (Inherent Risk Assessment) methodology to risk rank select third-parties
	Identifies tools and technology that can be used to automate processes
	Leverages an integrated view of risk across all risk domains
Level 5 Optimized	TPRM processes focus on continuous improvement
	Technology utilized to automate processes and provide real time reporting capabilities

Establish the Program

DEFINE YOUR GOVERNANCE AND OVERSIGHT

Governance

Level 1

Initial

- Need for a program has been identified; but not yet fully defined
- No formal or documented policies, standards and procedures

Level 3

Managed

- Program has been created and approved
- Approved policies, programs and procedures are established, but not fully operational
- Framework Identified and utilized as guideline for program

Level 5

Optimized

- Program regularly tested, measured and enhanced as needed
- Policies, standards and procedures reviewed annually and enhanced as needed
- Framework fully integrated regularly measured, tested and enhanced as needed

Setting Objectives and Goals

Importance of Clear Objectives

Clear objectives provide a roadmap for the third-party risk management program, ensuring focused efforts and effective risk handling.

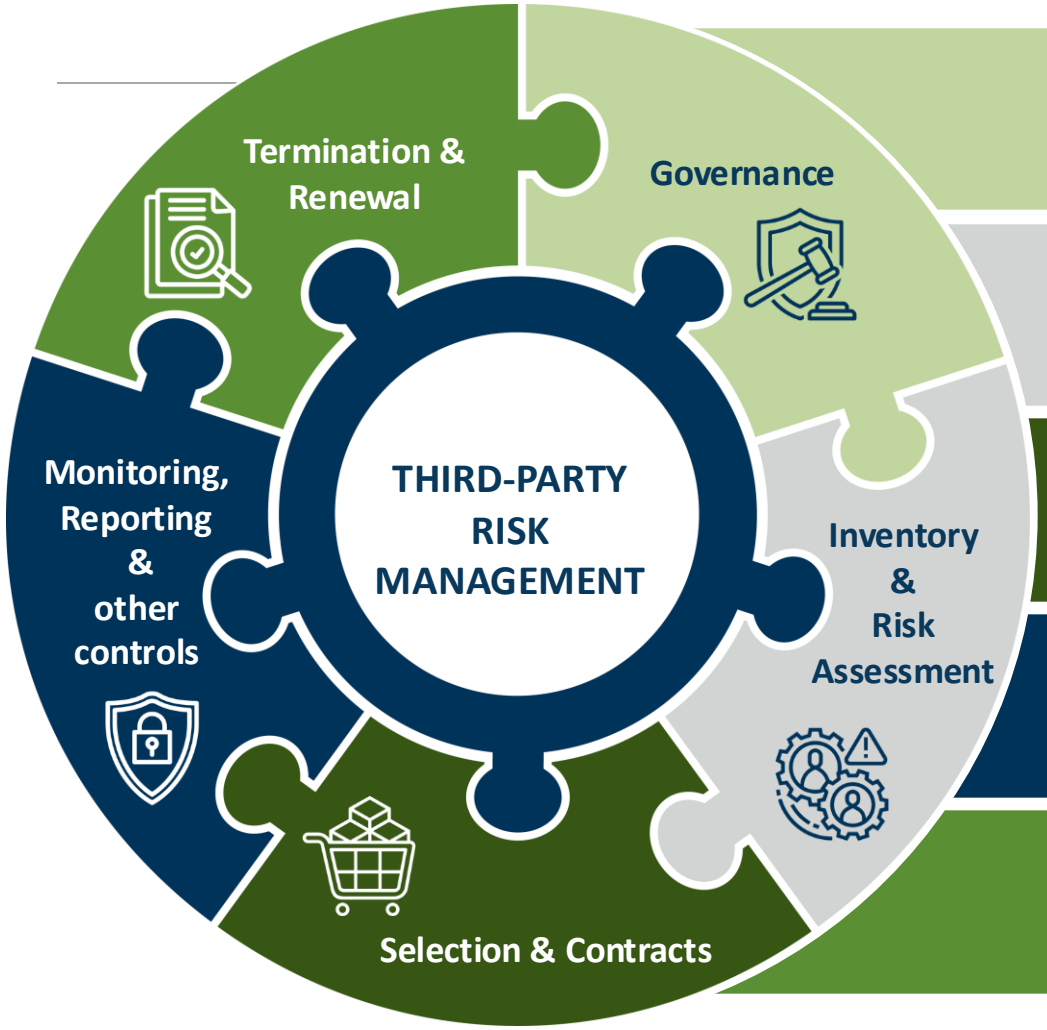
Alignment with Business Strategies

Objectives should align with overall business strategies to ensure coherence and effectiveness in risk management efforts.

Risk Appetite Consideration

Setting objectives must consider the organization’s risk appetite, balancing risk-taking with risk management.

Third-Party Risk Management Lifecycle



- Outsource Planning
- Strategic Direction
- Policies and Procedures

- Inventory
- Risk Assessments

- Selection & Bid Process
- Contracts

- Monitoring
- Periodic Reviews
- Reporting
- Internal Audits
- External Audits/Examinations

- Termination
- Renewals
- Renegotiations

Stakeholders & Roles

ADHOC → REACTIVE → PROACTIVE

Level 1

Initial

- Resources are contacted on adhoc basis
- Teams disconnected and working in silos
- Some knowledge, skills and expertise may be recognized but no formal positions or job descriptions exist

Level 3

Managed

- Resources have been defined and identified
- Collaboration of teams, some processes connected
- Staffing requirements defined. Some resources in place gaps have been identified but not all gaps have been resolved

Level 5

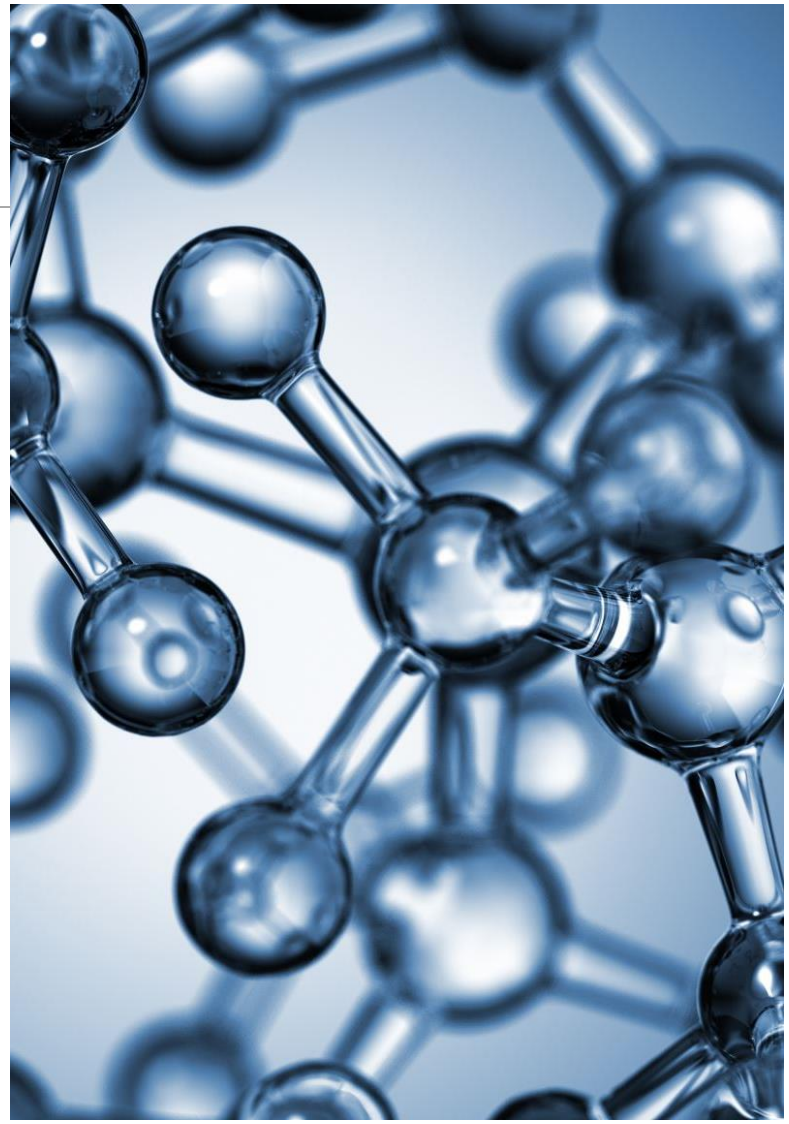
Optimized

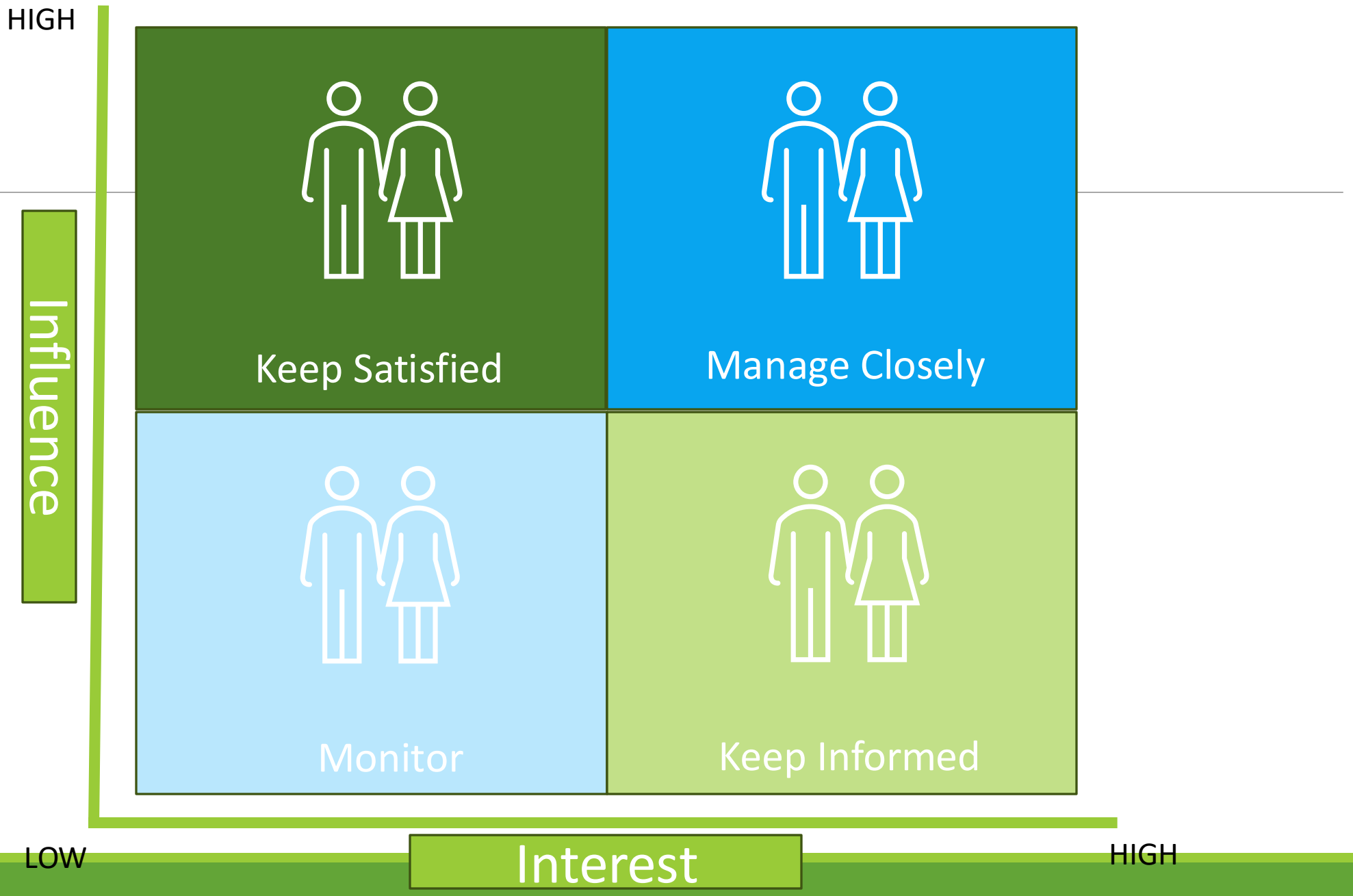
- Resources fully integrated into program
- Hybrid Model implemented where controls roll up into centralized program

Identify Your Stakeholders

Identify all the significant internal/external teams that your program may/will rely on for success. Examples of these organizations include:

- Information Security (cyber monitoring)
- Data Governance (data mapping, geolocational, legal)
- Procurement (business, financial, social, legal)
- Human Resources (background checks, drug screening)
- Business Continuity/ Disaster Recovery (testing , BIA analysis)
- Facilities Management (physical access)
- Legal (legal and business monitoring)
- Compliance (laws, standards, and aligned frameworks and guidance)
- Finance (Financials, Payments)




HIGH
Influence
Keep Satisfied
Manage Closely
Monitor
Keep Informed
LOW
Interest
HIGH

Implement and Manage

WHAT PROGRAM STRUCTURE IS APPROPRIATE YOUR ORGANIZATION

Inherent & Residual Risk

ADHOC → REACTIVE → PROACTIVE

Level 1

Initial

- Analysis is completed adhoc
- No standardized methodology

Level 3

Managed

- Defined Inherent & Residual risk questions, but no defined scoring methodology or model
- Assessed as part of purchase only

Level 5

Optimized

- Defined scoring methodology and model
- Inherent and Residual Risk questions reviewed annually and enhanced as needed
- Risk Re-assessed as part of periodic reviews
- Residual risk outcomes built into contracting process

Enhancing Risk Identification and Mitigation

Rigorous Assessment Techniques

Adopting more rigorous assessment techniques ensures a comprehensive understanding of potential risks involved in various projects.

Proactive Vulnerability Management

Proactively addressing potential vulnerabilities helps in mitigating risks associated with third-party relationships effectively.

Portfolio Stratification

Level 1

Initial

- One-time identification of third-parties
- Criticality has not been defined
- Third-party service classes not defined

Level 3

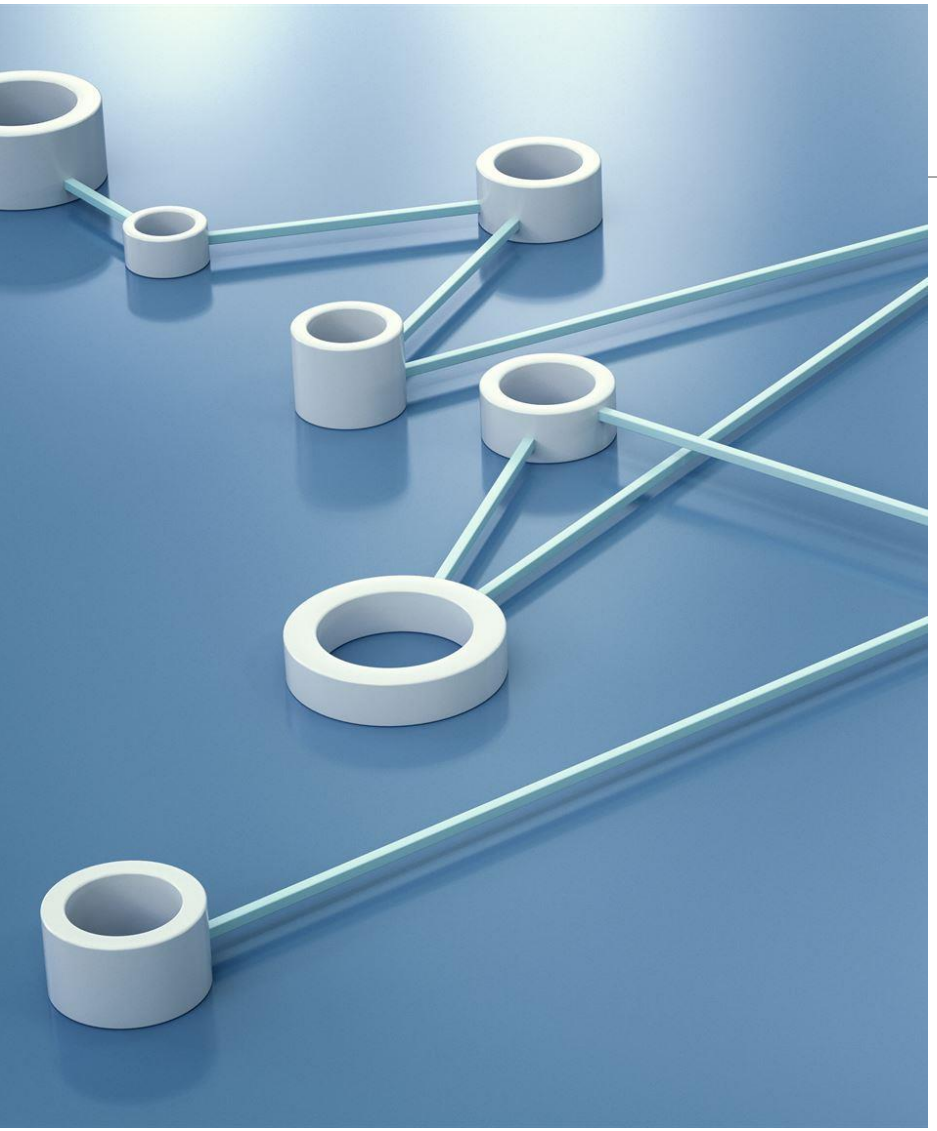
Managed

- Centralized repository
- Adhoc reports to identify third-parties
- High level service classes
- Criticality defined but inconsistently applied

Level 5

Optimized

- Criticality consistently applied
- Automated proactive reports to identify third-parties
- Identification of critical Nth Parties
- Service classes consistently allocated



Creating a Centralized Vendor Repository

SINGLE SOURCE OF TRUTH

A centralized vendor repository serves as a single source of truth for all vendor-related data, ensuring accuracy and consistency.

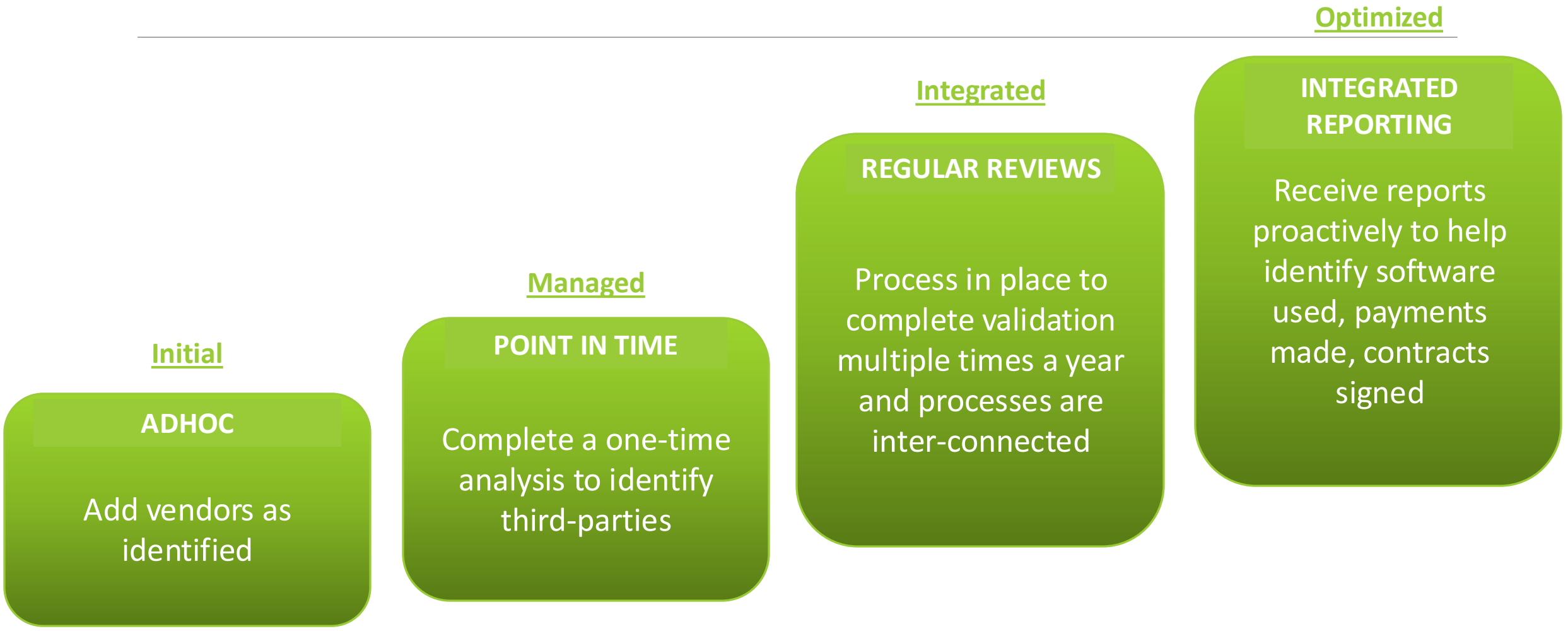
SIMPLIFIED RISK ASSESSMENTS

With all vendor information in one place, organizations can easily perform risk assessments, reducing potential vulnerabilities.

ENHANCED VISIBILITY

A centralized repository enhances visibility into third-party relationships, facilitating better decision-making and management.

Portfolio Stratification



Risk Assessment/Questionnaires

ADHOC → REACTIVE → PROACTIVE

Level 1

Initial

- Inconsistent questions
- One questionnaire used for all third-parties

Level 3

Managed

- Defined Risk Assessment criteria based on type of service
- Defined questionnaires allocated based on the risk
- Utilizing industry standard questionnaires, or using as comparison

Level 5

Optimized

- Defined Risk Assessment criteria based on type of service
- Pre-population of questionnaires utilizing documentation
- Annual review of questionnaires and enhance as needed

Due Diligence Questionnaire Maturity

Initial

ONE SIZE "FITS ALL

One (Usually long) questionnaire used to assess all vendors

Managed

MULTIPLE VERSIONS

Multiple questionnaires of varying lengths used to vet vendors in different tiers

Integrated

SELF SCOPING

A single, smart assessment that includes questions based on inherent risk and adjusts mid-assessment based on the vendors answers

Optimized

SELF SCORING

Smart assessment that pre-scores answers (good vs bad) and automatically generates issues and follow-ups to reduce review time

Due Diligence

The process of collecting information that provides management with the information to address all risk aspects of potential third-parties

Technology Service

- Cloud Provider
- Managed Email/Firewall/Network/Infrastructure
- Intrusion Detection/Prevention system (IDS/IPS)
- Internet service provider/Website provider

Due Diligence Required

- ✓ Financials or Annual report
- ✓ SSAE 16 Soc 2 Type 2 with actions due for exceptions
- ✓ Software Escrow
- ✓ BCP Summary
- ✓ DR Test Results with report on remediation & retest on failures
- ✓ Information Security Policy
- ✓ GLBA privacy statement
- ✓ Incident Management History with proof of remediation
- ✓ Regulatory Report of Examination (RoE)
- ✓ Insurance certificate (Liability and/or Errors & Omissions)
- ✓ Assurance that vendor conducts employee background checks
- ✓ Proof of 4th party monitoring

Consulting

- IT Auditors
- Information Security Risk Assessment Services
- Compliance Assessment Services (BSA, ACH, etc.)
- Benefits consulting
- IT Specialists
- External Penetration testing
- Internal Vulnerability Assessments

Due Diligence Required

- ✓ Financials or Annual report
- ✓ Information Security Policy
- ✓ GLBA Privacy Statement (possibly included in control)
- ✓ Liability insurance
- ✓ Assurance that vendor conducts employee background checks

Contracting and Selection

PROTECTING YOUR ORGANIZATION FROM LEGAL HARM

Selection & Contracts

ADHOC | REACTIVE | PROACTIVE

Level 1

Initial

- Contract standards and procedures are not formally defined
- Selection processes are not defined and inconsistent

Level 3

Managed

- All contract provisions have been approved, but not fully operational
- Define contract review team, but not fully aligned
- Defined who can sign a contract
- Selection process and templates created and approved, but not fully operational

Level 5

Optimized

- Processes reviewed annually, regularly measured, and enhanced as needed
- Team fully allocated
- Selection process consistently applied, and templates used
- Tool implemented to automate selection process

Contracts Review & Negotiation

The contract is the single most important control in the outsourcing process. Contracts are clearly written with specific details to provide assurances or performance, reliability, security, confidentiality and reporting. Contracts should address:

- Scope of arrangement, relationship, services, and specific responsibilities
- Performance standards (SLA, KRI, or KPI's)
- Use of sub-contractors
- Right to audit
- Service Level Agreements (SLA's) for Recovery Time Objective (RTO) & Recovery Point Objective (RPO)
- Dispute resolution, termination and assignment
- Indemnification and limitation of liability
- TSP updates (Regulatory or Federal information, memorandums, and legislation)
- Cost and compensation
- Confidentiality and Security
- Business resumption and contingency plans (BCP & DR)
- Exit strategy

Monitoring, Reporting & Other Controls

Monitoring & Reporting

ADHOC → REACTIVE → PROACTIVE

Level 1

Initial

- Tools, measurement and analysis are ad hoc and metrics are not yet fully defined
- Risk monitoring and evaluation activities are ad hoc and processes are not yet fully defined

Level 3

Managed

- Tools and analytics are established, but are not fully operational
- Metrics are measured on adhoc basis
- Monitoring tools established, but are not yet fully operational
- Periodic review are completed as needed

Level 5

Optimized

- Tools and analytics are established, and automated.
- Proactive metrics provide deeper insights into potential risks and trends.
- Monitoring tools fully operational and defined
- Periodic review completed on define frequency

Monitoring, Reporting & Other Controls

Monitoring

- QBR's with your Critical vendors
- Cyber Security Monitoring
- Adverse new monitoring
- Risk Monitoring
- OFAC & Sanction Monitoring
- Site Audits
- Performance Review

Reporting

- Board Reporting
- Program Efficiency Reports (KPI's & KRI's)
- Vendor KPI's
- Vendor KRI
- Geographic locations
- Data Breach
- Incident Response

Other Tools

- Internal Audits
- External Audits
- Regulatory Audits
- Self Assessments
- Maturity Assessments
- Control Reports

Developing Advanced Risk Analytics and Reporting

Insights into Vendor Risks

Advanced risk analytics allow organizations to gain deeper insights into potential vendor risks, enhancing their understanding of vulnerabilities.

Informed Decision-Making

With advanced analytics, organizations can make more informed decisions by evaluating risks comprehensively and strategically.

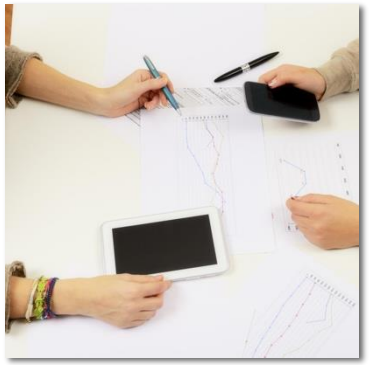
Effective Risk Mitigation Strategies

Organizations can develop effective risk mitigation strategies based on insights gained from advanced risk analytics, reducing overall risk exposure.

Conducting Regular Audits and Reviews

Importance of Regular Audits

Regular audits are essential to maintain the effectiveness of the TPRM program and identify potential weaknesses.



Identifying Areas for Improvement

Audits help organizations uncover areas that require improvement, fostering continuous development and better processes.

Ensuring Compliance

Regular reviews ensure that established policies are being followed, maintaining compliance and reducing risks.

Conclusion

Importance of Risk Management

Developing a robust third-party risk management program is vital for organizations to mitigate potential risks effectively.

Stages of Maturity

Following the outlined stages of maturity helps organizations systematically enhance their risk management capabilities.

Implementing Best Practices

Adopting best practices is essential for organizations to strengthen their resilience against third-party risks.