Thomas Bronack, President
Data Center Assistance Group, LLC
bronackt@dcag.com | bronackt@gmail.com
(917) 673-6992
https://www.dcag.com

Table of Contents

Contents

Table of Figures

The Problem

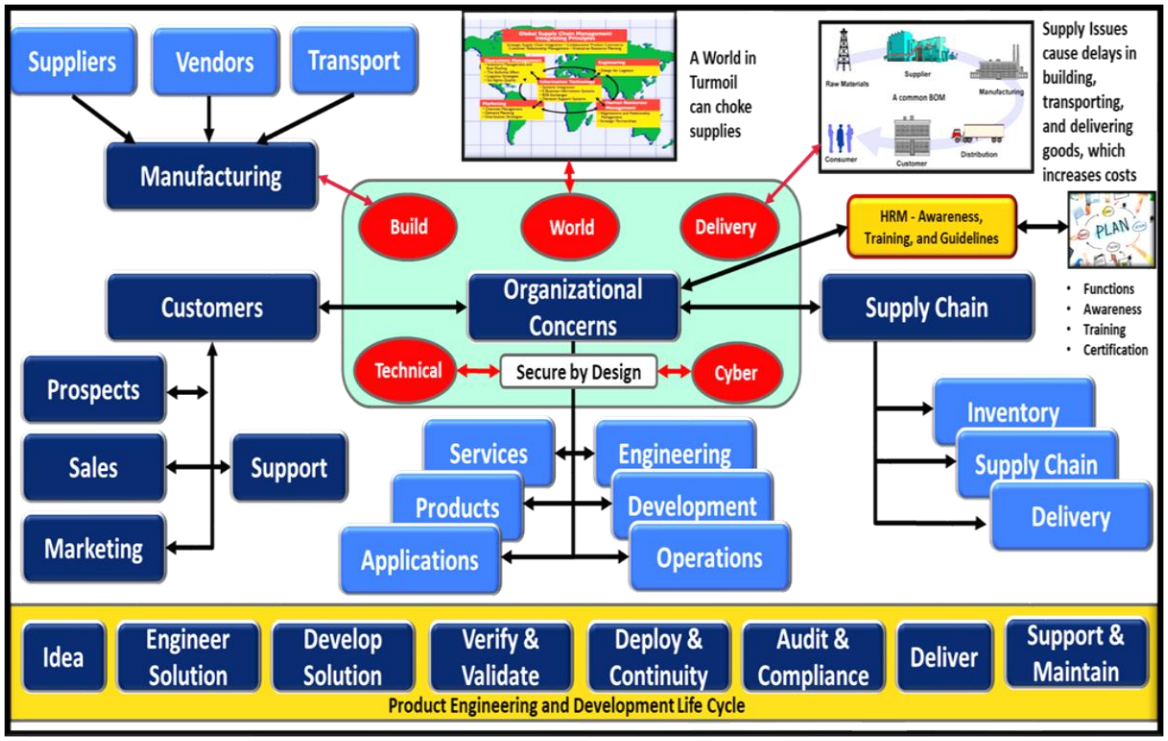

Figure 1: Why vendor and supply chain management is so important!

Vendor and supply chain management is a world-wide problem that is impacted by national conflicts, restricted travel, contagion, and other problems causing interruptions to delivery schedules, manufacturing, client delivery schedules, and IT service provision. This document addresses the needs associated with safeguarding your company against avoidable interruptions related to vendor and supply chain management.

The Solution

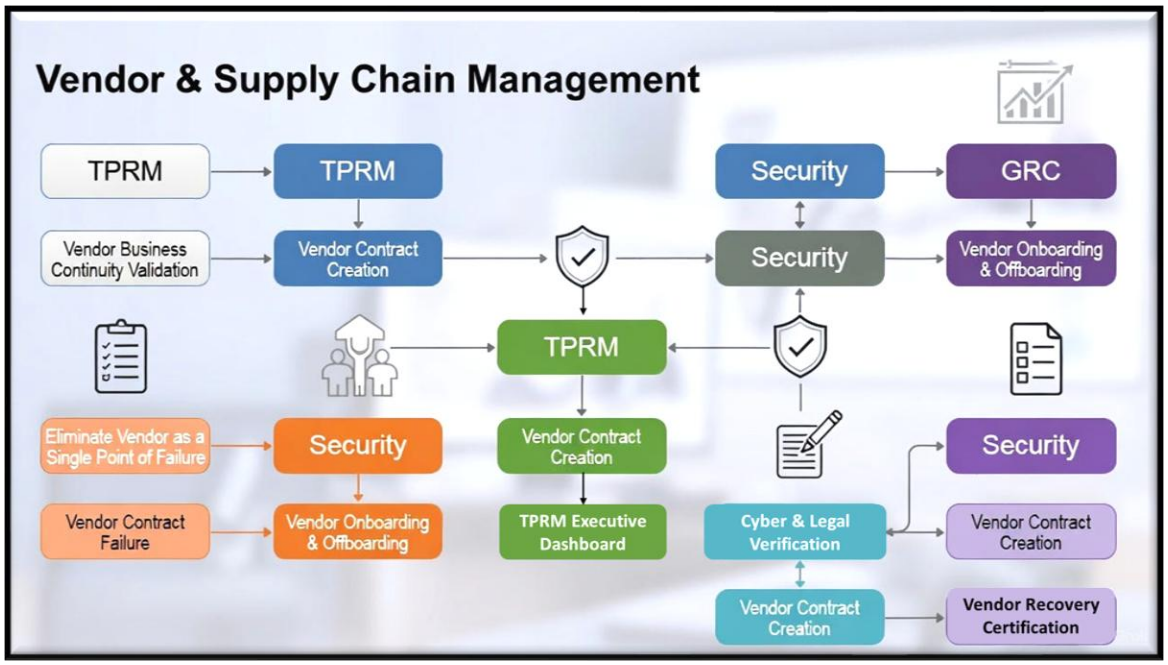

Figure 2: Vendor and Supply Chain Management with TPRM

This project description includes:

- Vendor and Supply Chain Management (worldwide understanding).
- Third Party Risk Management.
- TPRM Organizational structure and staff functional requirements.
- Awareness and technical training provided to stakeholders and technical staff.
- Security and technical problem identification, reporting, and mitigation.
- Compliance with domestic and international laws and regulations.
- Vendor identification (current and future).
- Analyzing, rating, and prioritizing vendor usage, with identified risks in Risk Register with POA&M to mitigate uncovered risks.
- Ability to pass audits and obtain letter of attestation for regulators.
- Creating a Vendor Contract with Service Level Agreement statement and penalties.
- Vendor certification to company policies and documentation requirements.
- Vendor onboarding and offboarding.
- Vendor monitoring, analysis, and reporting.
- Vendor data protection (from sensitivity, encryption/Post Quantum Cryptography, access management) through vital records management (backup and recovery).

Project will be performed in phases with management approval, backing, and continuous funding. Reporting will be divided into executive, management, and team categories, with data format and content delivered on predefined stages)

Agenda and Goals of a TPRM Process

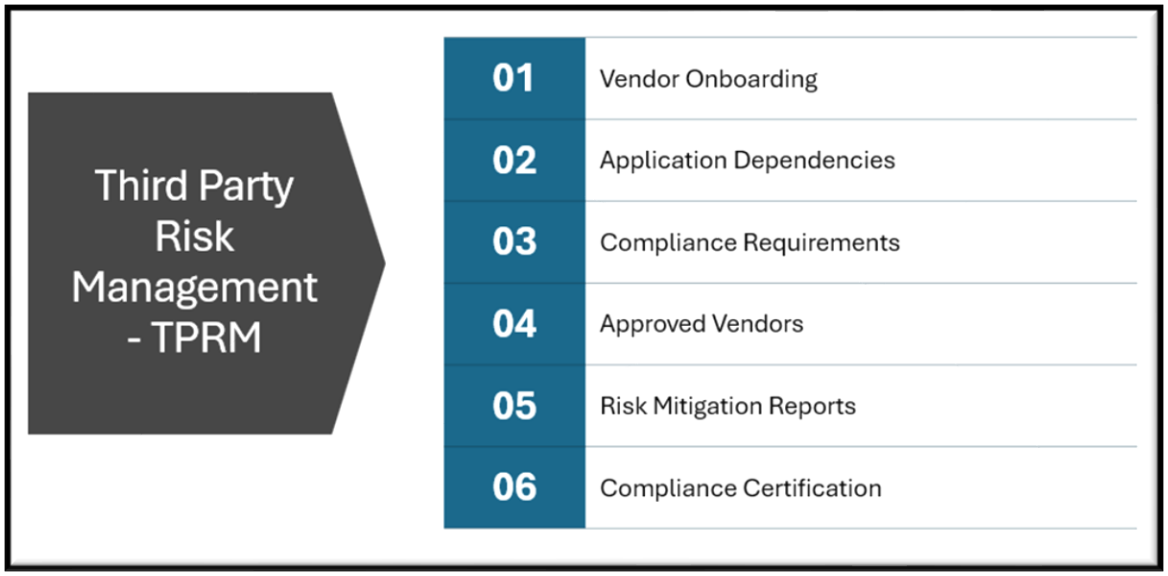

Figure 3: Goals of the TPRM Process

Project Overview:

This project is designed to identify vendor products within an organization's environment and to establish due diligence guidelines for vendor certification that are compliant with applicable national and international regulations and standards. Vendor product usage is assessed to determine criticality classification and recovery requirements.

Vendor recovery capabilities, and that they have an alternate delivery path to eliminate any single-point-of-failure they may be associated with. Contract provisions, monitoring and reporting implemented, and vendor onboarding and offboarding procedures defined.

Throughout the process, the current release levels of vendor products are systematically compared with those of existing installed products to address potential vulnerabilities. Compliance requirements for vendors are defined to enable formalized vendor approvals. Exceptions to vendor approval are documented in a vendor risk register, with a Plan of Action and Milestones (POA&M) established to mitigate identified risks.

Upon completion, compliance certification is issued to approved vendors, and a dashboard system is implemented for ongoing monitoring of vendor product status. This system generates risk reports to identify and guide the remediation of vendor anomalies.

Together, these measures create a stable environment underpinned by certified vendor products.

Legal, compliance, risk and procurement leaders, and problem/incident management can use this research to identify technology solutions and risk domains for managing and mitigating third-party risk. TPRM platforms offer versatile capabilities that support supply chain, IT, technical problem / cybersecurity incident mitigations, procurement, legal and compliance functions.

Mandatory Features

TPRM solutions must support the following activities:

- **Identifying third-party risk:** Determine which risk domains are relevant to a third party.
- **Analyzing risk:** Measure the potential impact on a customer's business or supply chain and provide an impact estimate.
- **Managing and escalating risk:** Offer platform functionality to surface and escalate risks, informing risk mitigation efforts. This may include escalation, tracking, action plans and risk categories.
- **Continuous monitoring:** Provide visibility into risk events through dashboards, reports, alerts, reminders and notifications.
- **Third- and fourth-party risk mapping and metrics:** Offer risk mapping, risk visualization, metrics and the ability to export third party risk data for reports and presentations.

Market Recommendations

- Build and scale the TPRM program by considering the entire TPRM life cycle. Ensure the TPRM platform facilitates the flow of third-party risk information across all relevant functions and users to maximize the organization's visibility of emerging third-party risks.
- Select a TPRM solution that is adaptable and scalable for both near-term and future program needs. When assessing TPRM technology options, ensure the organization has a "must have" list of capabilities prior to engaging with vendors.
- Evaluate the licensing options and consider both short-term and long-term implementation and integration requirements and APIs for the chosen TPRM solution provider, rather than solely focusing on cost.

Third Party Risk Management (TPRM)

Third Party Risk Management (TPRM) is a systematic process for identifying, assessing, managing, and monitoring risks from third-party vendors or service providers. It helps prevent external partners from introducing unacceptable risks to your operations or development processes. Executive Management must be aware of the vendors and controls in place to support business needs, safeguard continuity of services, protect revenue streams, and ensure compliance with relevant laws and regulations.

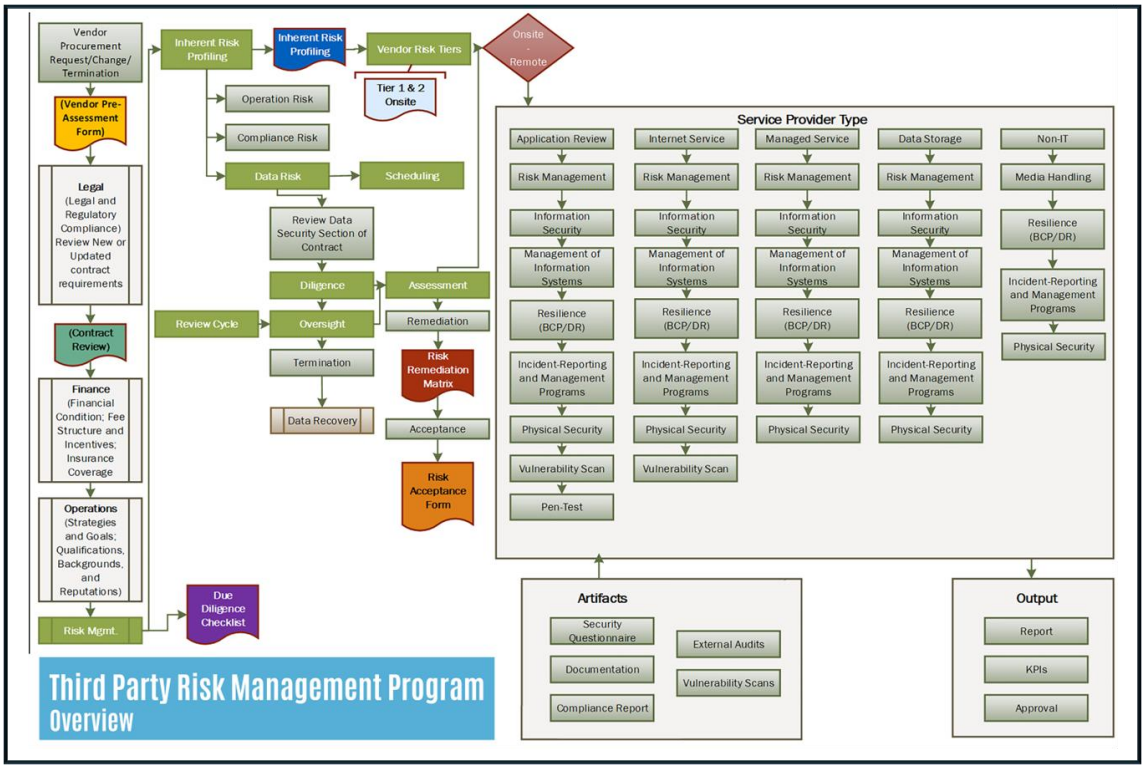

Figure 4: Overview of Thord-Party Risk Management process.

Purpose of This Document

This guide is intended for Technical Risk Management (TRM) Analysts and aims to provide a practical framework for implementing TPRM within the vendor and supply chain management phase of the application development process. The methodology balances technical, compliance, and executive oversight concerns.

Phase 1: Planning and Policy Definition

- **Goals: Define Compliance requirements and select Team Members.**
- Establish a TPRM governance structure.
- Define roles, responsibilities, and escalation paths.
- Develop and document third-party risk management policies and procedures.

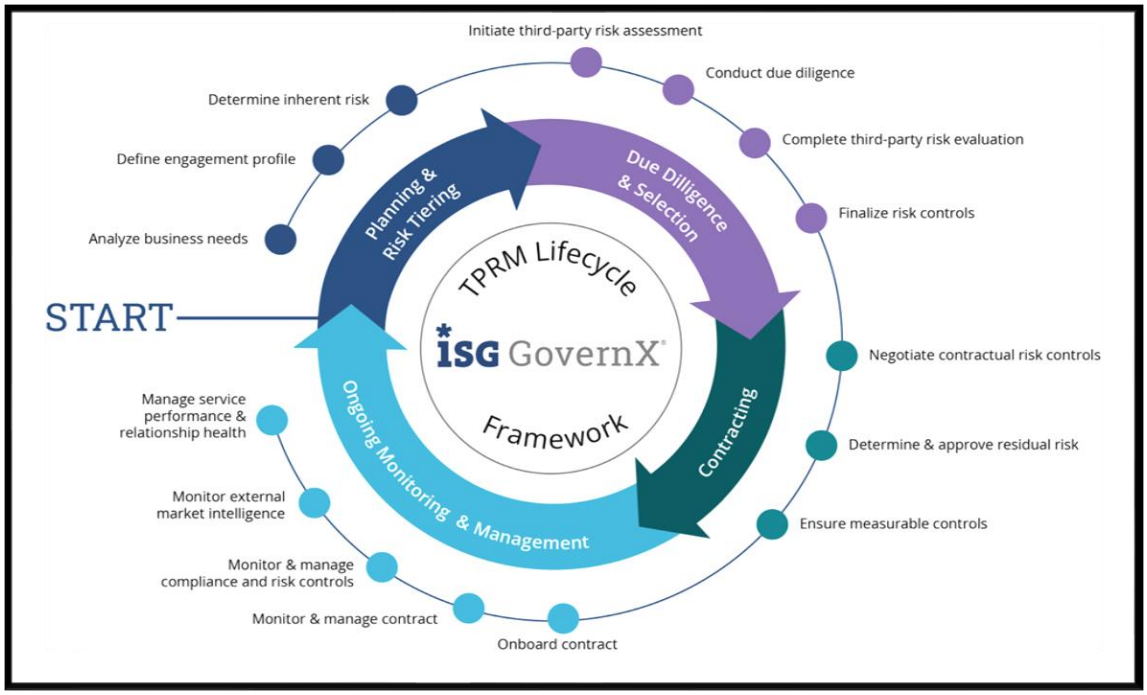

Figure 5: TPRM Governance Structure and Lifecycle Framework

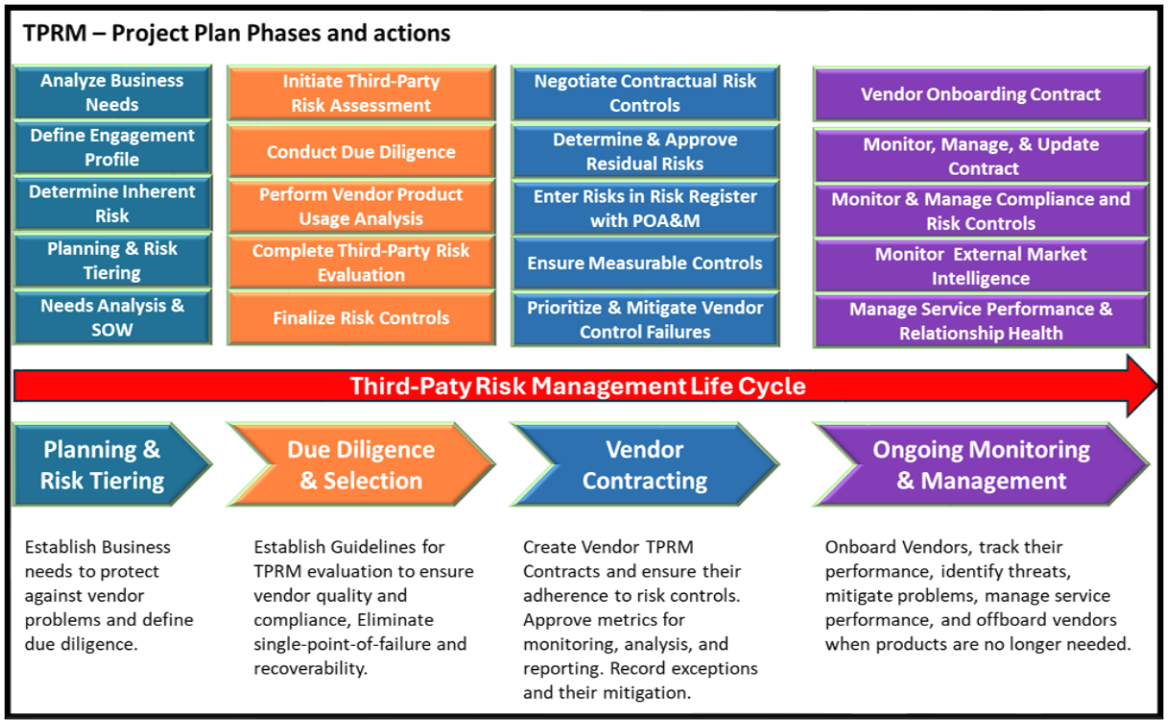

Figure 6: Third-Party Risk Management Life Cycle, phases and goals.

TPRM Governance Structure and Project Life Cycle								
		Planned		Actual				
Step:	Activity:	Start:	End:	Start:	End:	Performed By:	Percentage Completed:	Comments:
1	**Analyze Business Needs**							
a	Define Engagement Profile							
b	Determine Inherent Risk							
c	TPRM Planning & Risk Tiering approval							
d	Define Nees Analysis and Statement of Work							
2	**Initate TPRM Assessment**							
a	Conduct Due Dilligence							
b	Perform Vendor Product Usage Analysis							
c	Complete TPRM Assessment							
d	Finalize Risk Controls							
3	**Negotiate Contractual Risk Controls**							
a	Determenie & Approve Residual Risk							
b	Enter Risks in Risk Register with POA&M							
c	Ensure Measurable Conrols							
d	Prioritize & Mitigate Vendor Control Failures							
3	**Create Onboard Vendor Contract**							
a	Monitor & Manage Vendor Contracts							
b	Monitor & Manage Compliance and Risk Controls							
c	Monitor External Market Intelligence on Vendors							
d	Manage Service Performance & Reltionship Health							
e	Make improvements as deemed necessary							
f	Vendor Offboarding Procedures							

Figure 7: TPRM Governance Life Cycle Project Plan

Analogy: Think of this phase like drafting building codes before construction. You define what is acceptable, who enforces rules, and how safety is maintained.

Third-Party Risk Management Project Gantt

Third-Party Risk Management Project Plan - Actions, Purpose, Durations				
Step:	Action:	Purpose:	Days:	Project Steps
1	Planning & Policy	Establish Governance Framework	10	
2	Planning & Policy	Define TPRM Policy	7	
3	Vendor Inventory	Develop Vendor Inventory	6	
4	Vendor Inventory	Categorize Vendors by Risk	4	
5	Risk Assessment	Conduct Risk Assessments	10	
6	Risk Assessment	Collect Due Diligence Docs	7	
7	Contracting	Review & Update Contracts	8	
8	Contracting	Integrate Compliance Controls	6	
9	Monitoring	Setup Monitoring Tools	9	
10	Monitoring	Define KPI & Alerts	5	
11	Offboarding	Develop Offboarding Procedures	6	
12	Offboarding	Conduct Termination Risk Reviews	4	
			82	

Figure 8: TPRM Project Gantt Chart

Phase 2: Third-Party Inventory and Risk Classification

- **Goals: Identify Vendor Products, Contacts, and Rate Criticality.**
- Create a comprehensive inventory of third-party vendors.

- Categorize vendors based on risk tiers (e.g., critical, high, medium, low).
- Identify which vendors support critical application functions.

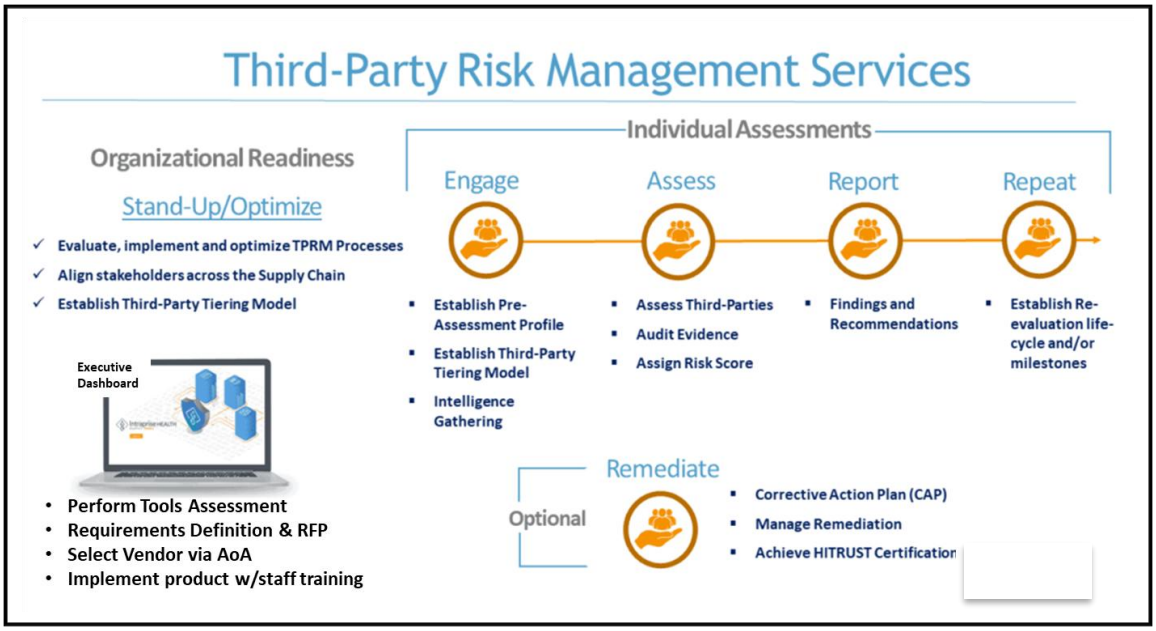

Figure 9: Third-Party Risk Management Services

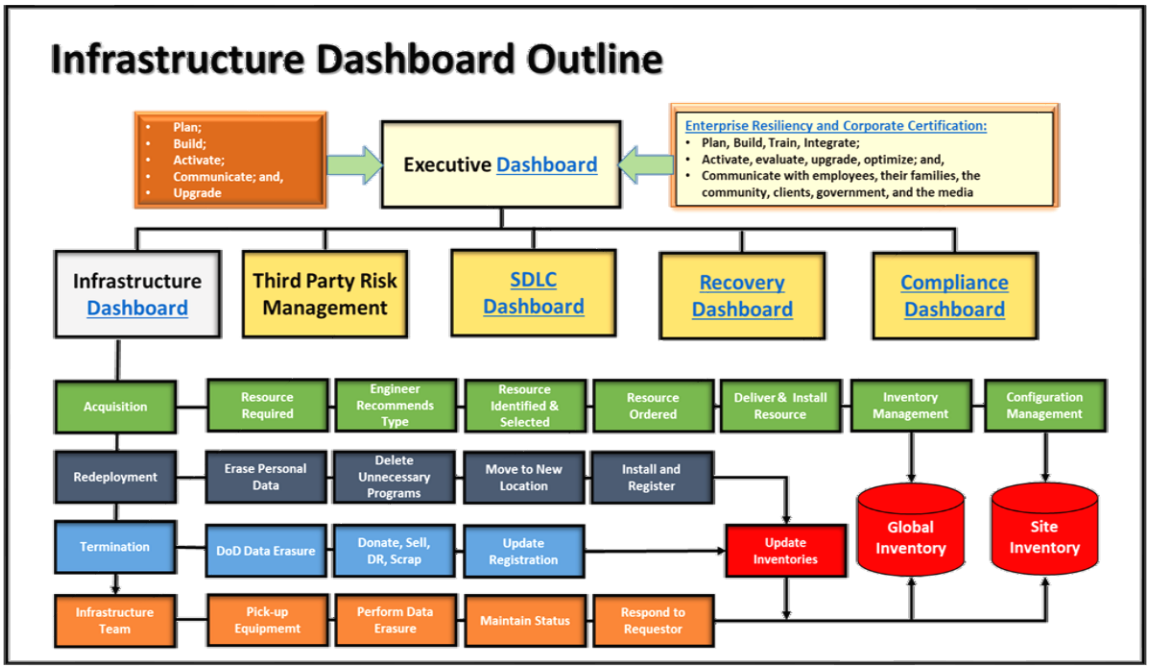

Figure 10: Inventory and Configuration Management

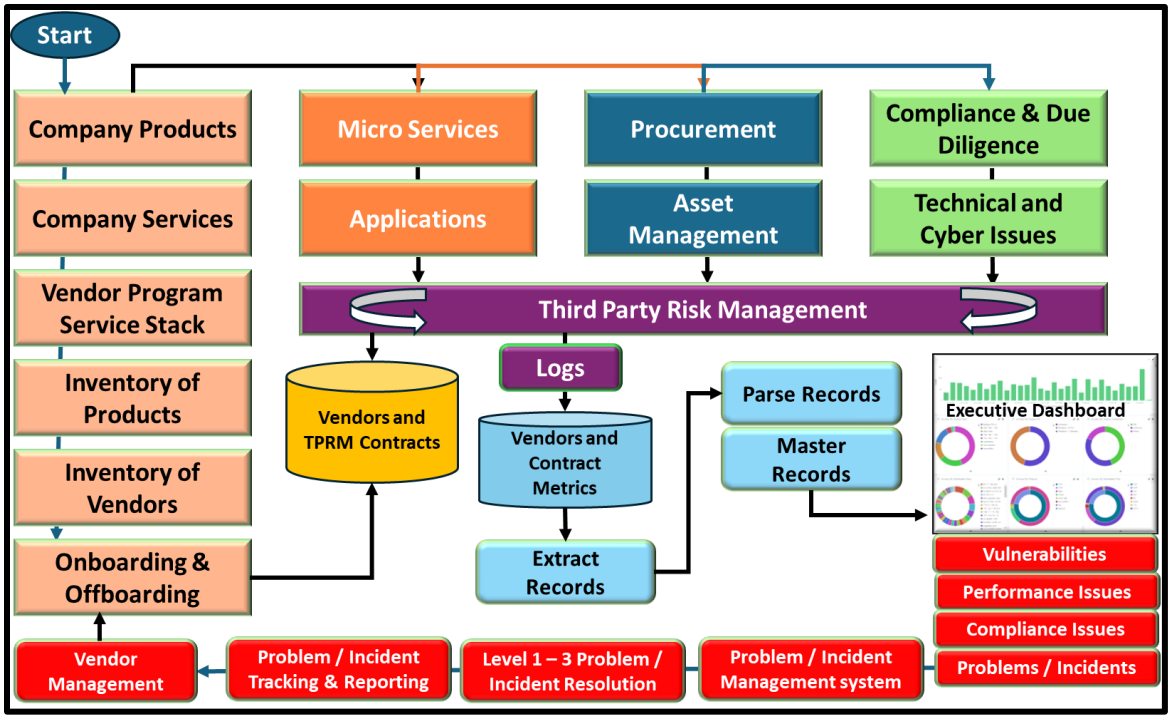

Figure 11: TPRM Actions from Inventory through Monitoring and Management

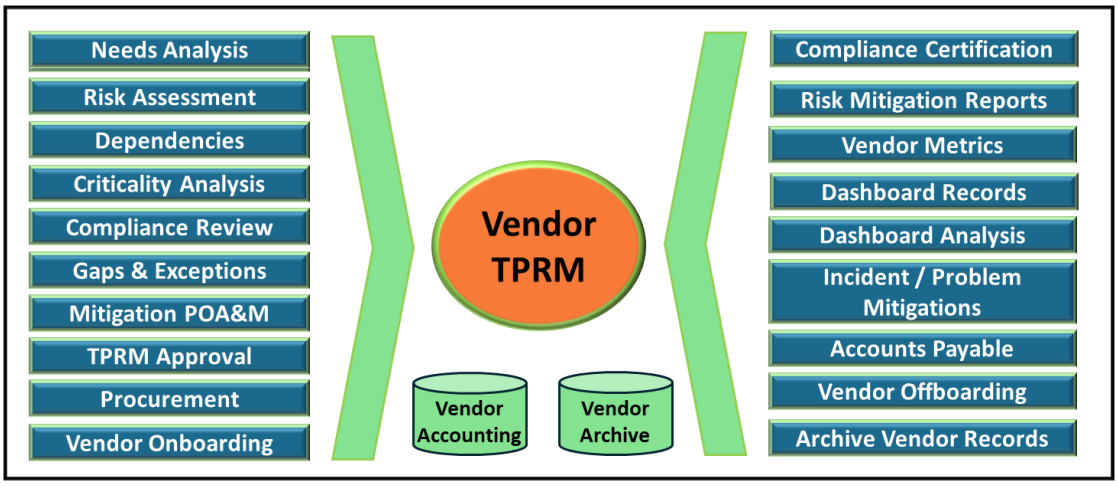

Figure 12: TPRM Vendor Certification Process

Analogy: Like triaging patients in an ER, you are prioritizing which third parties need urgent attention based on how risky they are.

Phase 3: Risk Assessment and Due Diligence

- **Goals: Conduct a TPRM Risk Assessment to define security conditions.**
- Conduct risk assessments including cybersecurity, compliance, operational, and reputational risks.
- Request and evaluate documentation (SOC 2, ISO 27001, questionnaires).
- Score vendors and flag unacceptable risks.

Figure 13: SOC 2 Overview - Trust Service Criteria

Analogy: This is like running a background check before hiring a contractor—you need to verify their track record, licenses, and ability to do the job safely.

Phase 4: Contractual Controls and Onboarding

- **Goals: Establish and document controls over vendor products and support.**
- Include required clauses in contracts: SLAs, breach notification, right to audit, compliance mandates.
- Integrate security requirements and reporting obligations into agreements.
- Ensure onboarding processes account for access controls and data protection.

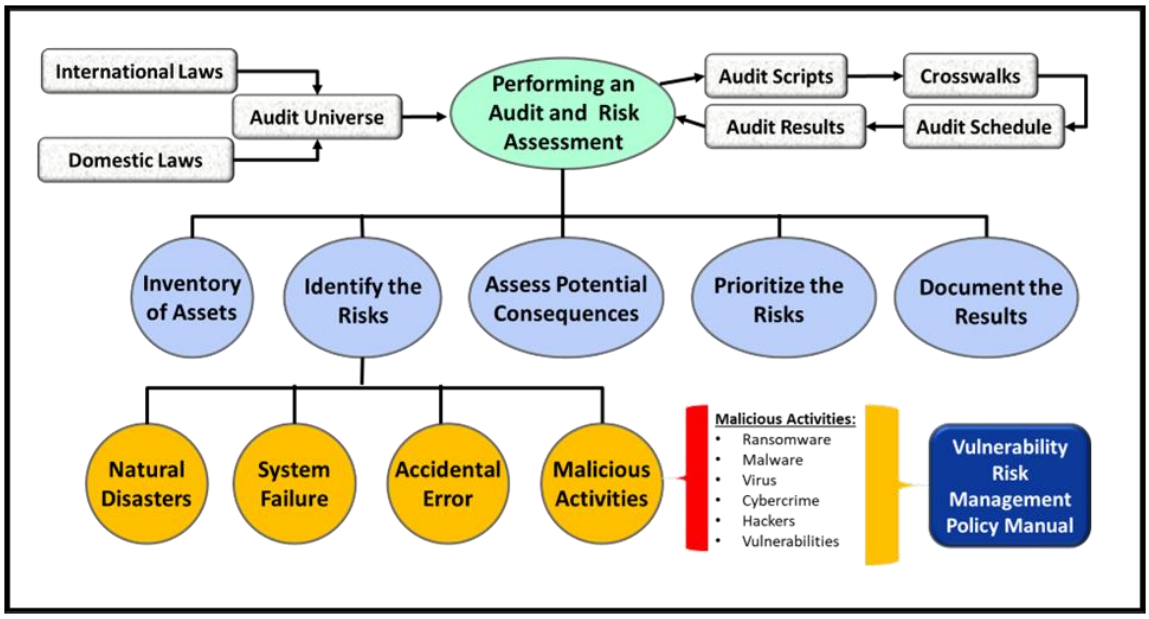

Figure 14: Performing a Compliance Audit for TPRM

Analogy: This is like buying insurance and setting expectations before handing over the keys to your house—you want legal protection in case something goes wrong.

Phase 5: Continuous Monitoring and Risk Mitigation

- **Goals: Provide a mechanism to continuously monitor the TPRM process, to detect and mitigate problems quickly and limit service interruptions.**
- Establish ongoing monitoring procedures using tools and KPIs.
- Define trigger events (e.g., breaches, financial downturns).
- Adjust risk ratings and mitigation steps based on performance and incidents.

An overview of the Continuous Monitoring and Problem Mitigation Process.

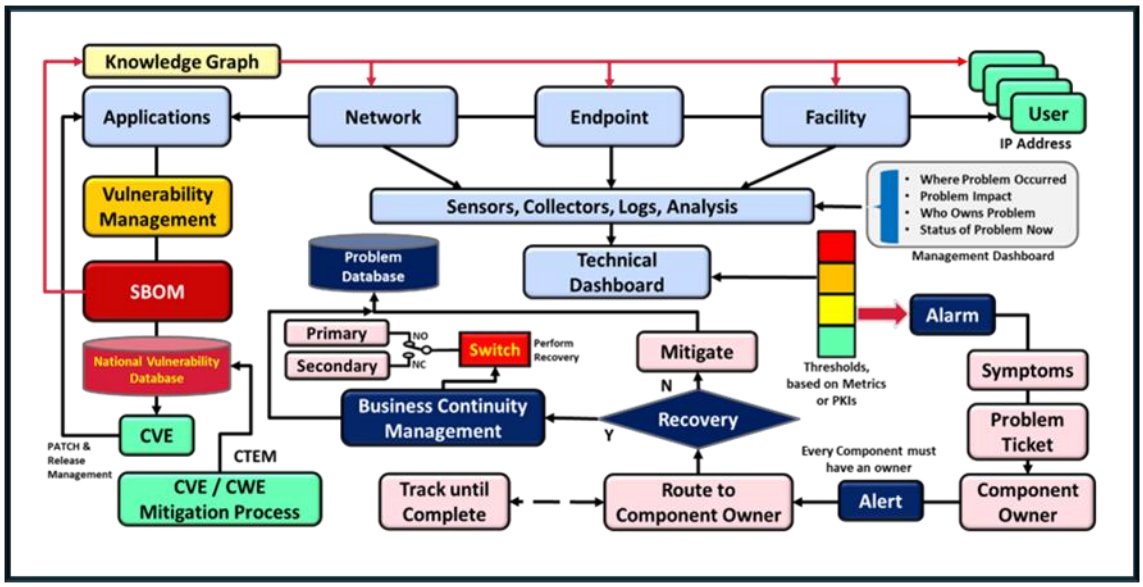

Figure 15:Continuous Monitoring and Reporting from a Dashboard

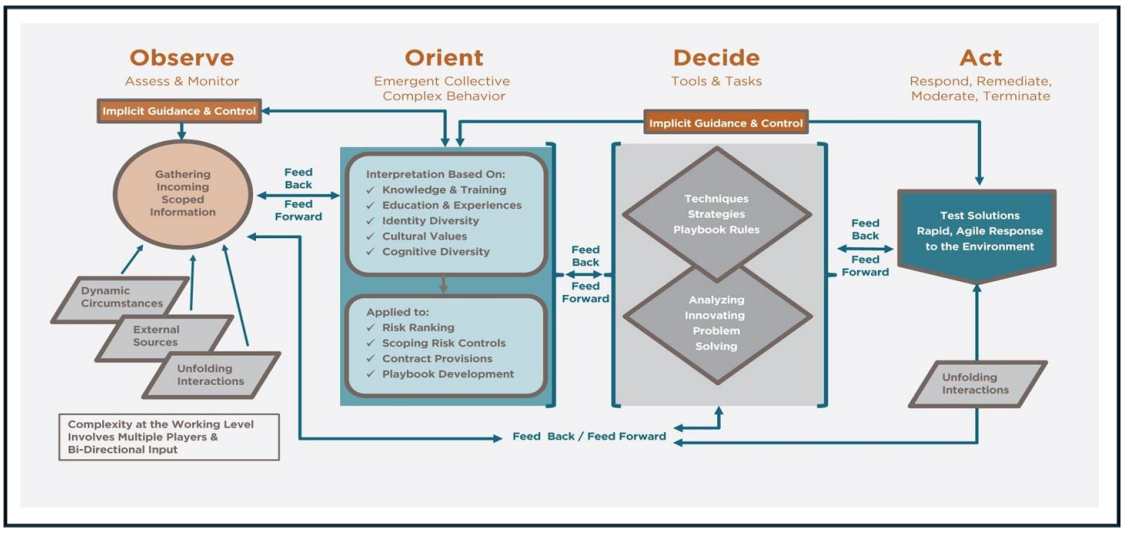

Figure 16: Developing and Using a TPRM Dashboard

Figure 17: TPRM Dashboard Functions for viewing.

Analogy: Like having security cameras and periodic inspections, this step keeps third parties accountable long after the contract is signed.

Phase 6: Offboarding and Termination Risk Management

- **Goals: To ensure Vendor Records are maintained in a current manner.**
- Ensure access is revoked and data is returned or destroyed.
- Conduct a termination risk assessment to prevent residual risk.
- Document lessons learned to improve future third-party management.

Vendor Offboarding Checklist areas of concern.

Follow the steps in this checklist when offboarding vendors from your organization.

1. Contractual Closure

- Review the vendor contract for termination clauses and obligations.
- Confirm all deliverables have been met.
- Ensure final payments are processed and documented.
- Terminate the contract formally and archive it.

2. Data Security & Intellectual Property

- Retrieve or securely delete all sensitive data shared with the vendor.
- Confirm destruction or return of proprietary information.
- Ensure compliance with data privacy regulations (e.g., GDPR, CCPA).

3. Access Revocation

- Disable vendor access to systems, applications, and networks.
- Revoke physical access to facilities or secure areas.
- Audit logs to confirm access termination.

4. Asset Recovery

- Retrieve company-owned equipment, credentials, or software licenses.
- Document returned assets and reconciled inventory.

5. Documentation & Reporting

- Maintain a detailed log of offboarding activities.
- Update vendor risk profiles and closure status in the TPRM system.
- Generate a final risk assessment report for audit purposes.

6. Stakeholder Communication

- Notify internal stakeholders (IT, Legal, Procurement, Security).
- Communicate the offboarding timeline and expectations to the vendor.
- Provide a point of contact for any post-offboarding queries.

7. Compliance & Legal Review

- Conduct a compliance check to ensure regulatory obligations are met.
- Involve legal counsel to assess any residual liabilities or risks.
- Document legal clearance and retain for future audits.

8. Lessons Learned & Continuous Improvement

- Conduct a post-offboarding review to identify process gaps.
- Update TPRM policies and procedures based on findings.
- Integrate feedback into future vendor lifecycle management.

Tailored Vendor Offboarding Checklist (TPRM-Aligned)

1. Contract Termination

- ☐ Review contract terms and termination clauses
- ☐ Confirm all deliverables are completed
- ☐ Process final payments and close purchase orders
- ☐ Issue formal termination notice

2. Data & Information Security

- ☐ Retrieve or securely delete all sensitive data
- ☐ Confirm destruction or return of proprietary information
- ☐ Audit vendor access logs for anomalies
- ☐ Ensure compliance with data privacy regulations (e.g., GDPR, CCPA)

3. Access Revocation

- ☐ Disable vendor access to systems, applications, and networks
- ☐ Revoke physical access to facilities
- ☐ Remove credentials from IAM systems

4. Asset Recovery

- ☐ Recover company-owned equipment and software licenses
- ☐ Reconcile inventory and document returned assets

5. Legal & Compliance Review

- ☐ Conduct legal review for residual liabilities
- ☐ Archive contracts, NDAs, and termination records
- ☐ Ensure regulatory obligations are met

6. Risk Management

- ☐ Update vendor risk profile in TPRM system
- ☐ Conduct final risk assessment
- ☐ Document offboarding risk mitigation actions

7. Operational Closure

- ☐ Decommission vendor-related services and integrations
- ☐ Confirm no dependencies remain in production environments
- ☐ Notify IT and procurement teams of service discontinuation

8. Stakeholder Communication

- ☐ Inform internal stakeholders (Legal, Security, Procurement, etc.)
- ☐ Provide vendor with offboarding timeline and expectations
- ☐ Assign internal point of contact for post-offboarding queries

9. Lessons Learned

- ☐ Conduct post-offboarding review

- ☐ Identify process gaps and improvement opportunities
- ☐ Update TPRM policies and procedures

Analogy: This is like changing your locks after a roommate moves out. You need to close all risk doors when the relationship ends.

TPRM Project Plan

This project plan outlines the major phases, tasks, durations, assigned personnel, estimated costs, and resource types required to implement a comprehensive Third-Party Risk Management (TPRM) program.

Third Part Risk Management Project Plan						
Step:	Phase	Task	Duration (days)	Assigned Role	Estimated Cost ($)	Resource Type
1	Planning & Policy	Establish Governance Framework	10	TPRM Program Manager	$10,000.00	Internal Staff
2	Planning & Policy	Define TPRM Policy	7	Compliance Officer	$8,000.00	Internal Staff
3	Vendor Inventory	Develop Vendor Inventory	6	Vendor Manager	$6,000.00	Internal Staff
4	Vendor Inventory	Categorize Vendors by Risk	4	Risk Analyst	$4,000.00	Internal Staff
5	Risk Assessment	Conduct Risk Assessments	10	Security Analyst	$9,000.00	External Consultant
6	Risk Assessment	Collect Due Diligence Docs	7	Compliance Officer	$7,000.00	Internal Staff
7	Contracting	Review & Update Contracts	8	Legal Advisor	$8,500.00	External Legal
8	Contracting	Integrate Compliance Controls	6	Compliance Officer	$6,500.00	Internal Staff
9	Monitoring	Setup Monitoring Tools	9	Monitoring Lead	$9,500.00	Tooling + Staff
10	Monitoring	Define KPI & Alerts	5	Security Analyst	$5,000.00	Internal Staff
11	Offboarding	Develop Offboarding Procedures	6	Procurement Officer	$4,500.00	Internal Staff
12	Offboarding	Conduct Termination Risk Reviews	4	TPRM Program Manager	$3,500.00	Internal Staff
	Totals:		82		$81,500.00	

Figure 18: TPRM Project Plan - Steps, Purpose, Length and Resources

This is a sample TPRM Project Plan that can be tailored to your specific organization.

Business Continuity Management

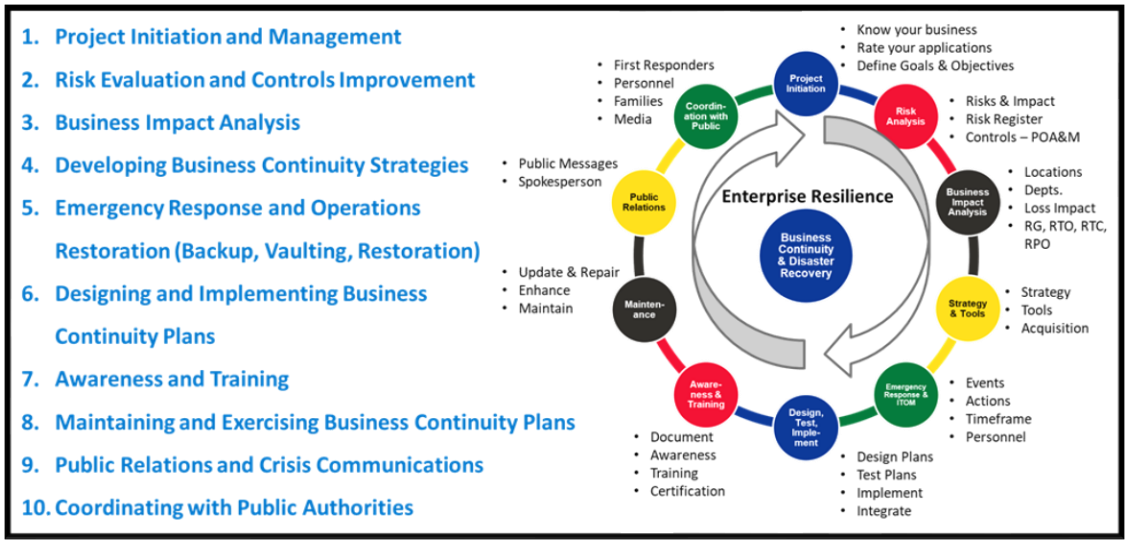

Figure 19: Business Continuity Management process.

Ten-Step process associated with Business Continuity and Disaster Recovery.

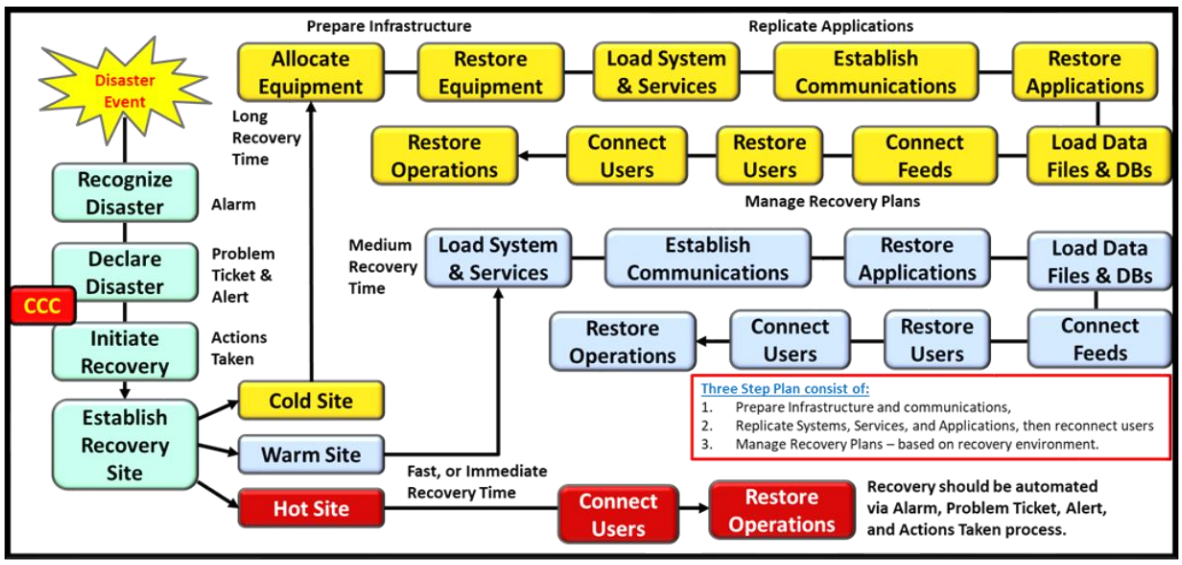

Figure 20: Disaster Recovery types of operations.

Flowchart of how to recover to a Hot, Warm, and Cold recovery site. A Hot site can recover instantaneously and is classified as Continuously Available (CA – Seconds to Minutes), a Warm Site can recovery in a predetermined time and is classified as High Availability (HA – Minutes to Hours), and a Cold Site is the slowest means of recovery as classified as Low Availability (LA - Days).

Revenue Loss Due to Lack of TPRM (Conceptual Graph)

Time Period	Incident Type	Impact	Estimated Revenue Loss
Q1	Vendor data breach	Regulatory fines, customer churn	$2.5M
Q2	Service disruption	Missed SLAs, lost contracts	$1.8M
Q3	Compliance failure	Legal penalties, audit costs	$1.2M
Q4	Reputational damage	Decline in customer trust	$3.0M

Figure 21: Revenue Loss due to not implementing TPRM.

Visual Chart of losses due to not implementing TPRM.

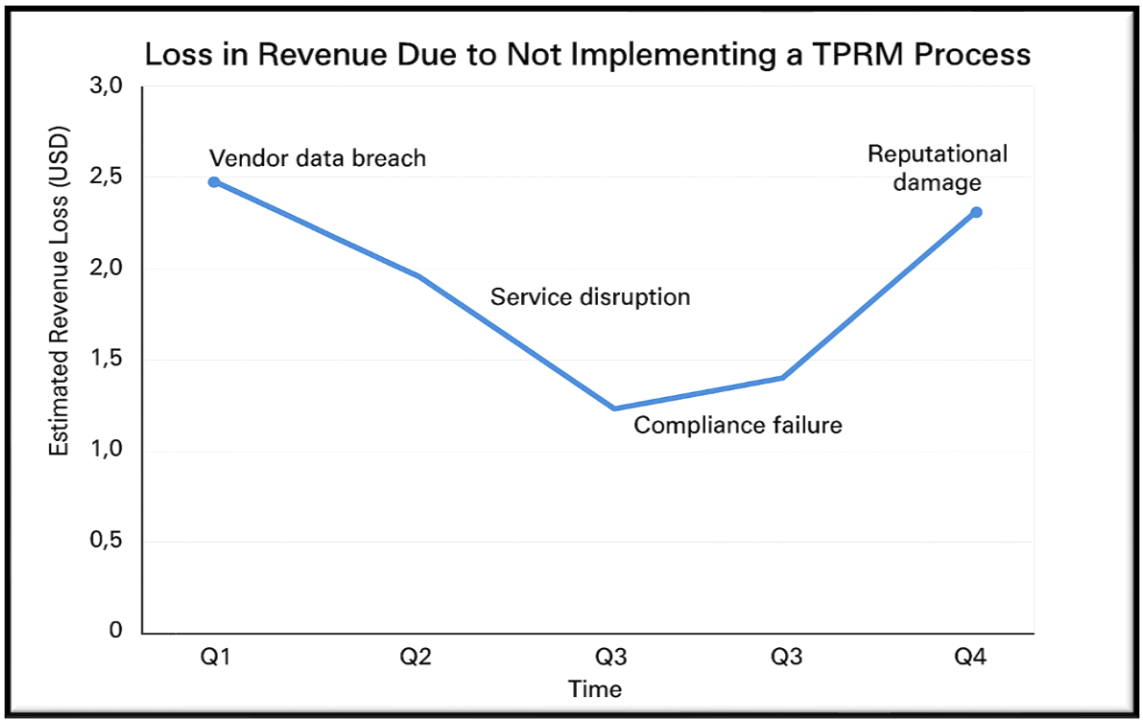

Figure 22: Visualization chart of Loss Revenue due to not implementing TPRM.

Cost vs Benefits analysis, by phase

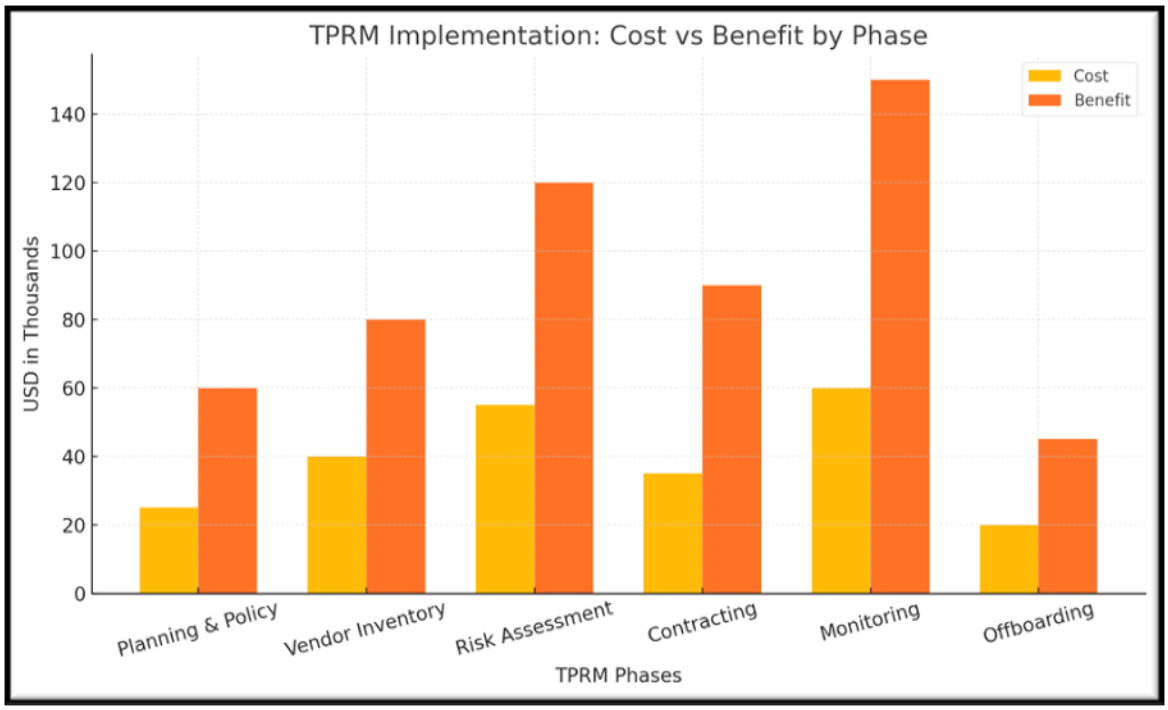

Figure 23: Cost vs Benefits Analysis, by Phase

This is comparison of costs for each phase of the TPRM Project, and the savings associated with the Benefits received by implementing TPRM. The next chart illustrates the Problem / Incident process.

Problems and Incident Management Lifecycle

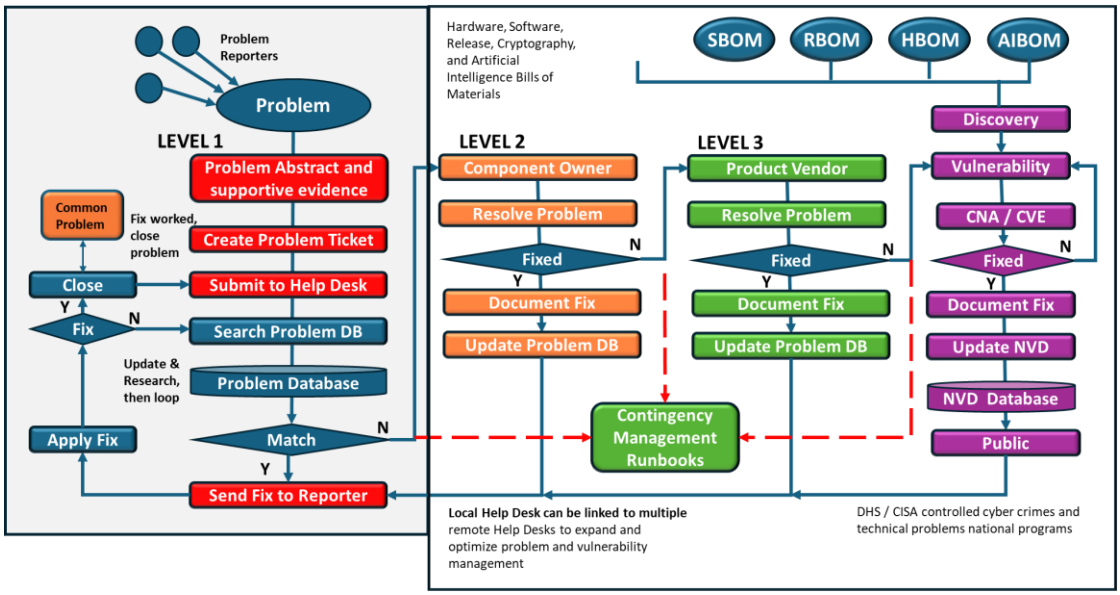

Figure 24: Problem and Incident Management System

United States TPRM Laws and Regulations, with links

United States TPRM Regulations		
Regulation / Guidance	**Description**	**Reference Link**
Interagency Guidance on Third-Party Relationships (SR 23-4)	Joint guidance from the Federal Reserve, FDIC, and OCC outlining risk management across the third-party lifecycle	Federal Reserve SR 23-4
Bank Service Company Act (BSCA)	Requires banks to notify regulators of third-party service contracts	Venminder Regulation Library
GLBA (Gramm-Leach-Bliley Act)	Mandates protection of consumer financial data, including third-party access	FTC GLBA Overview
CCPA (California Consumer Privacy Act)	Regulates third-party data sharing and consumer opt-out rights	CCPA Compliance Handbook
SOX (Sarbanes-Oxley Act)	Requires controls over financial reporting, including third-party risks	SOX Overview
HIPAA	Applies to third-party vendors handling protected health information	HHS HIPAA Guidelines

Figure 25: United States TPRM Laws and Regulations, with links.

International TPRM Laws and Regulations

International TPRM Laws and Regulations, with links		
Region / Regulation	**Description**	**Reference Link**
EU – GDPR (General Data Protection Regulation)	Requires data processors (third parties) to comply with strict privacy standards	GDPR Official Site
EU – DORA (Digital Operational Resilience Act)	Establishes ICT risk management standards for financial entities, including third-party oversight	Venminder Regulation Library
EU – EBA Guidelines on Outsourcing	Sets governance expectations for financial institutions outsourcing critical functions	European Banking Authority
Canada – OSFI B-10	Requires federally regulated financial institutions to manage third-party risks	OSFI Guideline B-10
UK – FCA Outsourcing Rules	Financial Conduct Authority guidance on outsourcing and third-party risk	FCA Handbook
Singapore – MAS Guidelines	Monetary Authority of Singapore's expectations for outsourcing risk management	MAS Guidelines
ISO/IEC 27001	International standard for information security, including third-party controls	ISO 27001 Overview

Figure 26: International TPRM Laws and Regulations, with Links

Six Key Steps to Strengthen Third-Party Risk Management (TPRM)

Introduction This section supplements the existing TPRM Guide by expanding on six critical operational pillars required to fully implement an effective TPRM program. Each step provides goal-driven instructions, implementation actions, supporting analogies, and references to guide staff and executives.

Figure 27: TPRM Six Pillars and Base Steps

1. Vendor Onboarding: Identifying Vendors & Products + Release Verification

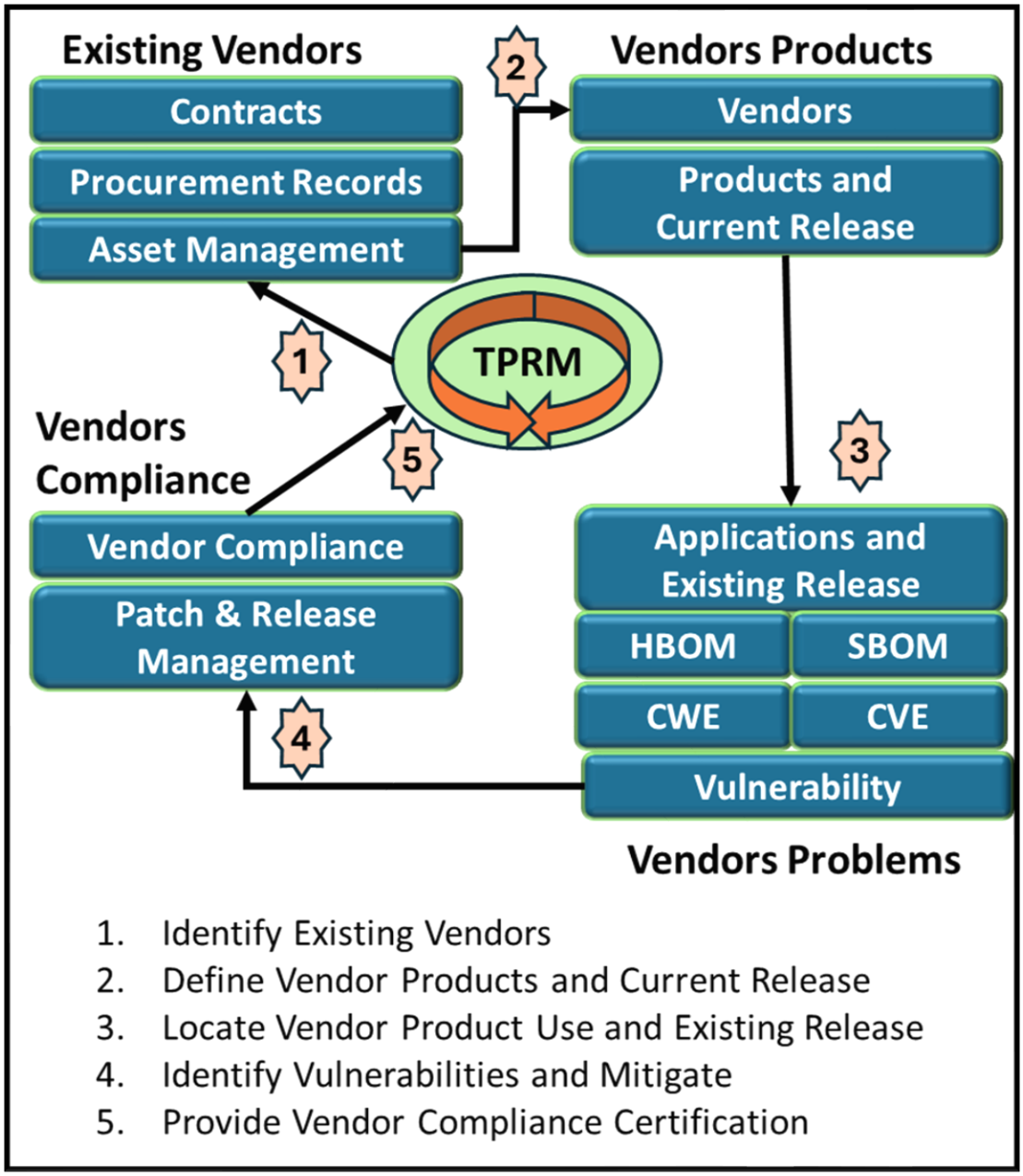

Figure 28: TPRM Stages and Action Steps

Goal: Establish a comprehensive onboarding framework to inventory vendors, identify supported products, and assess the technical currency of all vendor software.

Actions:

- Extract vendor information from contracts, procurement records, accounts payable systems, and asset management platforms.
- Identify all software, hardware, services, and tools delivered by each vendor.

- Use Configuration Management Database (CMDB) tools (e.g., ServiceNow, BMC Remedy, RSA Archer) to match vendor products to assets and services in production.
- Perform a version scan of all deployed products and compare them with vendor-maintained Current Supported Releases (CSR).
- Use HBOMs and SBOMs to identify vulnerabilities (CWE, CVE, etc.).

Tools:

- Nessus, Qualys, Lansweeper, or internal software inventories
- Identify End-of-Life (EOL), End-of-Support (EOS), or vulnerable versions.
- Document all findings into the vendor profile.

Analogy: Like inspecting the parts on an aircraft before flight, you must confirm the equipment is up to spec, not just present.

References:

- NIST SP 800-128 (Configuration Management)
- Vendor release catalogs (e.g., Cisco, Microsoft Lifecycle pages)

2. Application Dependencies: Mapping Vendors to Applications

Goal: Document and maintain visibility over which internal applications depend on third-party vendors to prioritize remediation, onboarding, or offboarding decisions.

Actions:

- Perform application dependency mapping using:
- Configuration Management Systems (CMS)
- Static/dynamic code analysis (e.g., Sonatype, Black Duck)
- Interviews with application owners and DevOps teams
- Maintain a matrix linking: Application Name → Function → Dependent Vendor → Product Version → Hosting Environment
- Tag critical systems for high priority onboarding and continuous monitoring.

Analogy: Understanding application dependencies is like knowing which beams in your house are load bearing before making renovations.

References:

- ISO/IEC 27001 Annex A.12.1.3 (Capacity management)
- OWASP Dependency-Track

3. Compliance Requirements: Verifying Regulatory Alignment

Goal: Ensure that vendor products comply with applicable laws, regulations, and standards relevant to your industry and geography.

Actions:

- Determine applicable regulatory frameworks:
- HIPAA, SOX, GDPR, CCPA, FedRAMP, PCI-DSS, NIST 800-53, etc.
- Map vendor responsibilities against control families (e.g., encryption, logging, data retention).
- Request compliance documentation (SOC 2, ISO/IEC 27001, FedRAMP ATO, SIG Questionnaire).
- Engage Legal, Compliance, and Risk teams to validate compliance assertions.
- Track regulatory requirements in a compliance matrix.

Analogy: Like ensuring a building has passed fire code inspections before opening to the public.

References:

- NIST 800-37 Risk Management Framework
- SIG Questionnaire (Shared Assessments)

4. Approved Vendors: Due Diligence and Approval Workflows

Goal: Standardize the process to evaluate, approve, and onboard vendors after assessing their risk profile and compliance maturity.

Actions:

- Develop and enforce a vendor intake workflow:
- Request for Information (RFI)
- Vendor Risk Assessment Questionnaire
- Financial viability and reputation review (Dun & Bradstreet, Moody's)
- Security assessments (penetration test results, SOC 2, etc.)
- Score vendors against pre-defined acceptance criteria.
- Submit evaluation results to a governance board (Procurement, Legal, Security, Compliance).
- Maintain an "Approved Vendors List" with rationale and expiration date.

Analogy: Like conducting background and credit checks before entering a business partnership.

References:

- ISO/IEC 27036 (Information security for supplier relationships)
- Gartner TPRM Best Practices

5. Risk Mitigation Reports: POA&M Documentation

Goal: Record, track, and resolve vendor-related risks through formalized Plans of Action & Milestones (POA&M).

Actions:

Log identified vendor risks in a central TPRM register.

- For each risk:
- Assign severity and owner.
- Define remediation actions.
- Set due dates and status updates.

Use a POA&M template that includes:

- Risk Description.
- Remediation Plan.
- Responsible Party.
- Target Completion Date.
- Residual Risk Rating.

Escalate overdue or high-severity risks to Governance Committees.

Include POA&M dashboards in regular risk review meetings.

Analogy: Like a construction punch list—clearly documented, assigned tasks that must be completed before sign-off.

References:

- DHS POA&M Template (https://www.cisa.gov/)
- FedRAMP Continuous Monitoring Guide

6. Compliance Certification: Verifying & Monitoring Ongoing Adherence

Goal: Continuously validate vendor compliance through documentation review, audits, and dashboards.

Actions:

Collect proof of compliance:

- Audit reports (SOC 2 Type II, ISO 27001).

- Certificates of insurance.
- Penetration test results.
- Data protection agreements.
- Track expiration and renewal timelines.
- Set reminders and trigger auto-escalation for expired certifications.

Display compliance status in dashboards:

- Green = Verified.
- Yellow = Due for Review.
- Red = Expired / Non-Compliant.

Analogy: Like keeping track of a vehicle inspection certificate—you need to verify it is still valid and has not lapsed unnoticed.

References:

- Shared Assessments VRMMM
- NIST CSF v2.0
- Microsoft SSPA Program

Vendor Lifecycle and TPRM Controls Overlay

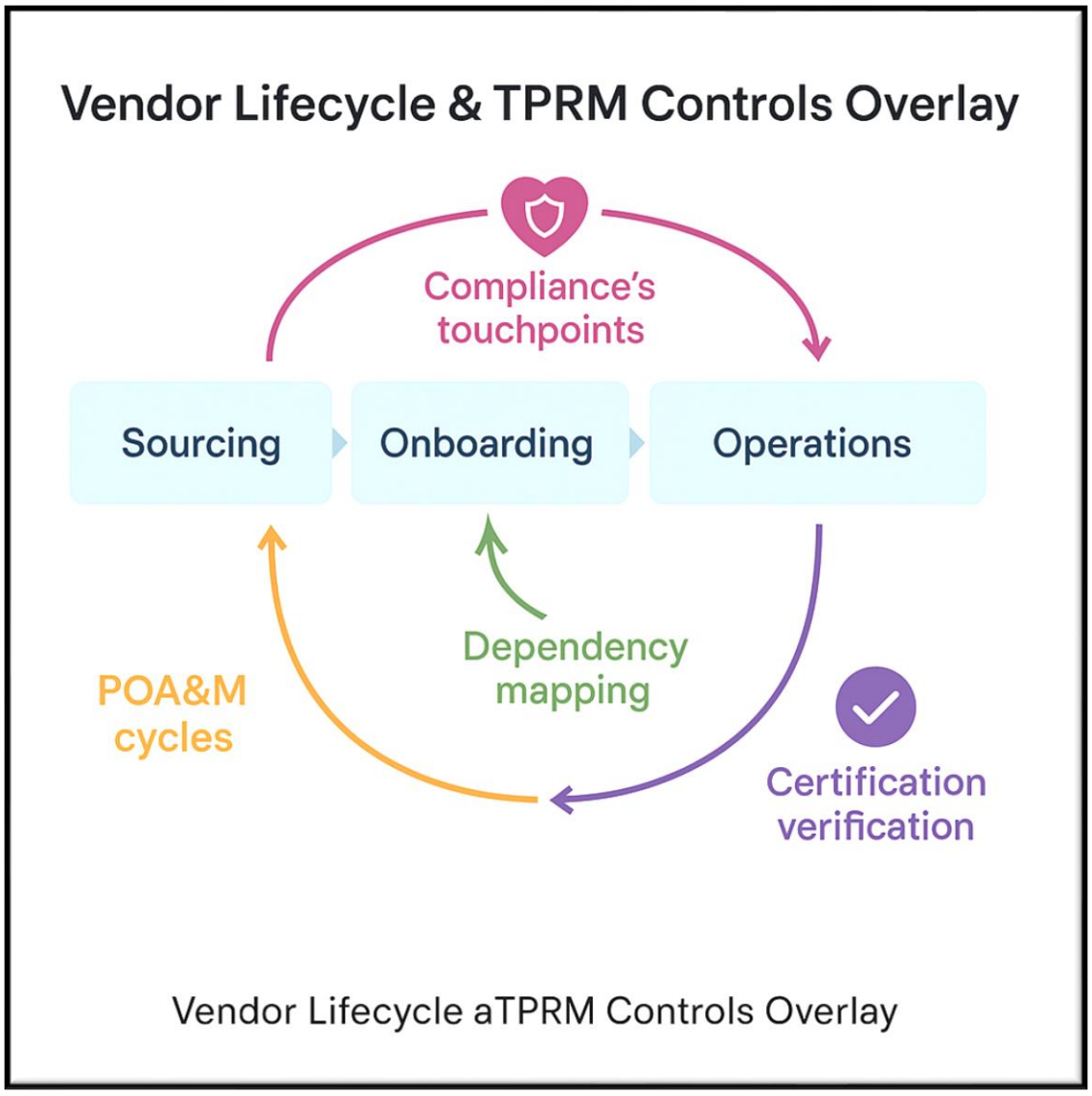

Figure 29: Vendor Lifecycle and TPRM Controls

References and Source Material:

1. NIST SP 800-161 Rev.1: https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final

2. ISO/IEC 27036 Supplier Security Guidance: https://www.iso.org/standard/59648.html

3. FedRAMP Continuous Monitoring Strategy Guide

4. Shared Assessments Program: https://sharedassessments.org/

5. Gartner TPRM Playbook: https://www.gartner.com/en/articles/third-party-risk-management

6. Ponemon Institute 2023 TPRM Study: https://www.riskrecon.com/ponemon-report-data-risk-in-the-third-party-ecosystem-study

Third-Part Risk Domains and Definitions

Risk Domain	Definition
Bribery and corruption	The risk of individuals or organizations engaging in unethical or illegal activities, such as offering or accepting bribes, gain an unfair advantage. This includes the risk of third parties engaging in bribery or corruption when conducting business.
Business Continuity	The evaluation of business resilience to disruptions, including disaster recovery and business continuity plans.
Business Governance	The risk of business failure, fines or pecuniary loss due to various financial risks such as credit downgrades, insolvency, inadequate financial controls, accounting irregularities, money laundering, lack of compliance with regulations, fraud, money laundering, terrorist financing or bankruptcy.
Capacity	The inability to deliver required products, services or personnel due to production or resource constraints.
Concentration	The risk is associated with using third parties located or operating in a specific geographic area or relying on services from the same subcontractor or fourth party. It also refers to the volume of work provided by a specific vendor or service provider.
Environmental, Social and Governance (ESG)	Metrics and principles used to assess enterprise nonfinancial performance data aimed at meeting disclosure requirements and complying with legislation and regulations across ESG focus areas such as carbon, environmental impact, labor relations, modern slavery, human rights, sustainability and ethical sourcing.
Geographic or geopolitical	Risks associated with services or products fulfilled outside the client's home country or region, including geopolitical risks, climate or natural disasters, currency fluctuations, legal or regulatory issues, resource availability (including human capital), or infrastructure-related risks.
Privacy and data processing and management	The risk of unauthorized access, misuse or loss of personal or sensitive data, including Personally Identifiable Information (PII), that the company stores, collects, or processes as a "data processor." This may

	involve potential violations related to the management of personal data, such as location, collection, processing, access, retention, return and destruction. Compliance with the General Data Protection Regulation (GDPR) is an example.
Regulatory Compliance	Government or industry-body-mandated obligations and requirements that third parties must comply with, including monitoring and reporting obligations. This includes accessibility, conflict materials or minerals, the Bank Secrecy Act (BSA) anti-money laundering (AML), know your supplier (KYS), know your customer (KYC), U.S. Securities and Exchange Commission (SEC) disclosure and reporting requirements, and other regulatory or legal obligations.
Security or cybersecurity	The risk of malicious cyberattacks or threats. It examines the physical and cyber technologies and processes that protect digital or information assets against malicious attacks or threats, and the responses to these events to minimize harm.

TPRM Monitoring and Reporting

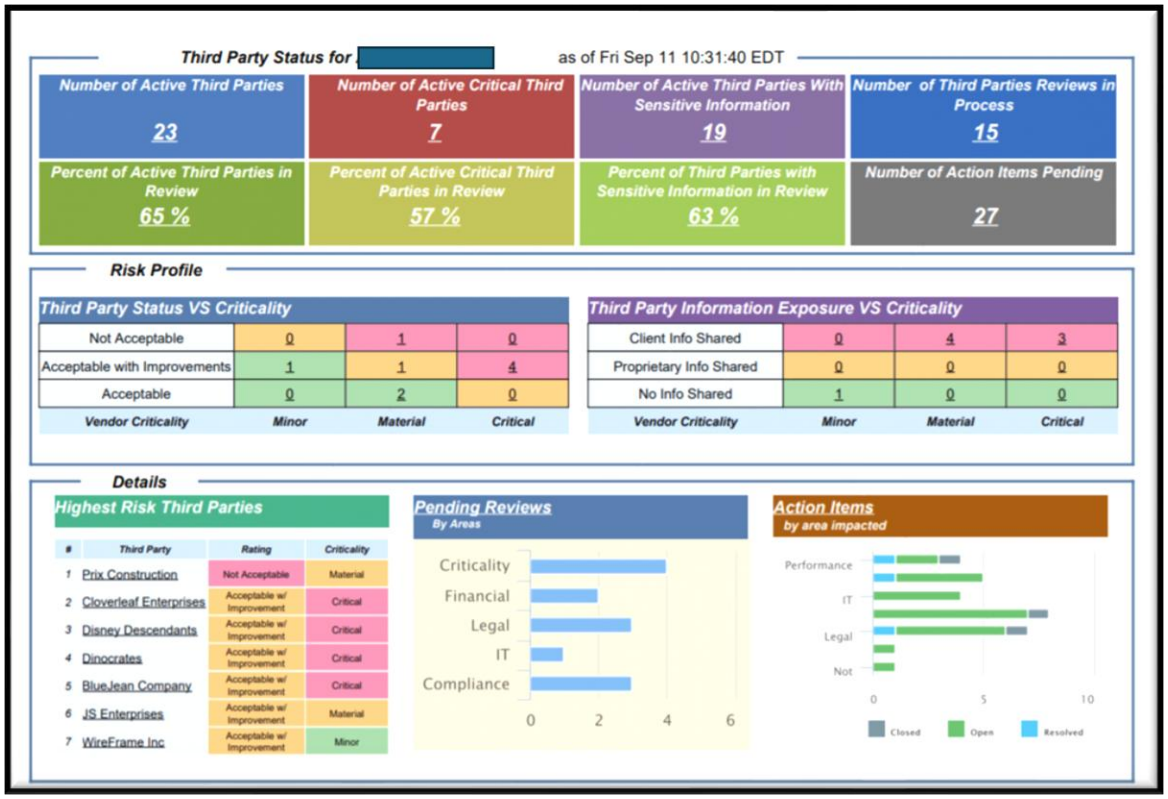

Figure 30: Third Party Risk Management Display Screen – Example

This is an example of a TPRM Dashboard, but your dashboard can be modified to best server your needs and in the language best suited to your culture.

Call to Action

To implement these six pillars effectively, organizations need a coordinated effort across Procurement, Legal, Security, Compliance, and DevOps. Contact Data Center Assistance Group, LLC for expert guidance on developing your TPRM ecosystem.

Thomas Bronack, president
Data Center Assistance Group, LLC
bronackt@dcag.com | bronackt@gmail.com
(917) 673-6992
https://www.dcag.com

