



Building Third Party Risk Management Program from Scratch

CHARMI PATEL – VICE PRESIDENT, HEAD OF VENDOR RISK MANAGEMENT

ISRAEL DISCOUNT BANK OF NEW YORK

This presentation expresses my personal view and not that of my employer Israel Discount Bank of New York

Rate your TPRM Program

2

CONTINUOUS PROGRAM IMPROVEMENT

MATURITY

- Informal, ad hoc approach
- Decentralized manual process
- Lack of senior management support

Needs Improvement

- Single resource / small team
- Manual questionnaire reviews and due diligence distribution
- Little to zero Senior management or Board involvement

Fair

- Dedicated team with a formally defined program
- Inherent risk calculations
- Somewhat defined TPRM framework
- Periodic reporting to Board
- GRC tool for third-party lifecycle management
- Developed due diligence standards

Satisfactory

- Dedicated team & available external resources
- Frequently active Board involvement
- Fully automated processes
- Systems interconnections
- Full visibility into supply chain lifecycle
- Comprehensive reporting
- Contracts management with SLA alignment
- Continuous program enhancements

Well-Controlled

TIME

You Might Have

- ▶ Few years old list of vendors with least possible information
- ▶ Not fully executed contracts, not sure of end dates and majority are auto renews
- ▶ Little to no bandwidth for ongoing monitoring activity
- ▶ Lack of communication between third-party program due diligence teams
- ▶ Business non compliance with TPRM
- ▶ Vendor classification is not consistent across the board

Key process to Build TPRM Program

- ▶ Vendor Selection/Planning
- ▶ Due diligence and onboarding
- ▶ Contract Negotiation
- ▶ Vendor monitoring
- ▶ Offboarding
- ▶ Escalation Process
- ▶ Develop KPI and KRI
- ▶ Handling consumer complaints
- ▶ Report an incident process
- ▶ Process for watchlist

Key Stakeholders for TPRM Program

- ▶ Board
- ▶ Senior Management
- ▶ Operational and Enterprise Risk Office
- ▶ SOX Office
- ▶ Finance and Planning Partners
- ▶ Procurement
- ▶ Office of General Counsel
- ▶ Information Security Office
- ▶ Business Continuity Office
- ▶ Risk and Compliance
- ▶ Data privacy officer
- ▶ Credit Risk officer

Key Technologies for TPRM Program

- ▶ A GRC tool or Specific TPRM tool
- ▶ Data Intelligence providers for cyber security, financial health, ESG
- ▶ Tools for OFAC/negative News/Sanctions screening

Calculate Inherent Risk

LOW <i>0 - 25</i>	25 Service is essential to company operations	5 Service is subject to regulatory requirements
MEDIUM <i>25-50</i>	20 Third party has access to Non public Information	5 Third party communicate to the Organization's client
HIGH <i>50-75</i>	20 Third party has access to technical infrastructure	5 Service is delivered as a cloud-based solution
CRITICAL <i>75-100</i>	5 Difficult to replace service with alternative	5 Third party require upfront payment or overspend is >5M
	5 Service can damage reputation significantly	5 Third party outsources a portion of the service

Due Diligence and Vendor Selection

- Information Security Officer
- Business Continuity Officer
- Credit Risk Officer
- Compliance Officer
- Data privacy Officer
- Office of General Counsel
- Procurement officer

Enrich and Streamline Third-Party Reviews

- Follow the industry best practice for due diligence process
- NIST, ISO, SIG questionnaire can help determine the vendors control to mitigate cyber security, business continuity risk
- OFAC, negative news, PEP should be identified and reviewed as part of compliance review
- Audited financial statements or data intelligence tool can determine vendor's financial health

Ongoing Monitoring Activities

Business Owners

- Complete vendor scorecard
- Assess vendor strategic direction and future road map
- Escalate vendor incidents
- Partner with TPRM for upcoming renewal
- Notify in change of service/product

Due Diligence Teams

- Assess vendor's security and risk controls from their respective areas
- Continuously monitor third parties on data intelligence tools
- Escalate risk/issues identified during reviews
- Periodic review on their TPRM procedure review to be aligned with applicable regulations

TPRM Office

- Periodically meet with vendors and business
- Contract management and track key data such as upcoming renewals, CPI increase, etc.
- Maintain subcontractors/4th party tracker
- Periodic review of TPRM framework. Policy and process
- Monitor, remediate and report the issues

Key Performance Indicators

- ▶ Average time to onboard a vendor
- ▶ Vendor Risk Assessment Completion rate
- ▶ Vendor renewal rate
- ▶ Outstanding periodic reviews
- ▶ Open number of internal audit finding
- ▶ Open number of Regulatory finding
- ▶ Significant operational incident causing customer complaints and financial loss
- ▶ Number of internal operational incidents

Reporting for Board and Senior Management

KPIs and KRIs are the good starting point for reporting to Board and Senior Management

▶ Senior Management

Tailored reporting for each individual head

Number of outstanding reviews by their team

Concentration risk in their supply chain

Percentage of vendor compliance to SLA

▶ Board

Overview of critical vendors and their risk posture

Extended vision for supply chain and nth party

TPRM future roadmap and strategic initiatives

Updates on open internal/regulatory findings

New critical or high risk vendor onboarding

Q & A

THANK YOU