Point of View - Third Party Risk Management
Deloitte Touche Tohmatsu India LLP
May 2018
How will you get ROI on your time investment today?

1. From VRM to TPRM to EERM – Demystifying the jargon

2. CxO speak - Why is it a Regulator / Board Room conversation?

3. What is the way to deal with this Elephant in the room?

4. Help!! - What are the technology and tools that are available?

5. What’s new – What should I look out for?
Demystifying the jargon
The Extended Enterprise

The extended enterprise is the concept that an organization does not operate in isolation. Its success is dependent upon a complex network of third party relationships.
### TPRM Framework covers....

<table>
<thead>
<tr>
<th>Drivers and Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third party Vulnerability</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scope of Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial performance</td>
</tr>
<tr>
<td>Liquidity</td>
</tr>
<tr>
<td>Profitability</td>
</tr>
<tr>
<td>Funding</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Monitoring and Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approach and Methodology</td>
</tr>
<tr>
<td>Self Assessment</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

© 2018 Deloitte Touche Tohmatsu India LLP.
CxO speak – Why is it a Boardroom / Regulator conversation?
Why do organizations need third party risk management capabilities?

Seven out of ten respondents believe that risks inherent in managing their extended enterprise have increased at least by some extent if not significantly. However, organizational self-assessment of their overall levels of EERM maturity continues to improve at a slow pace.

53 percent of respondents now believe that their journey to achieve the desired state of EERM maturity is two to three years or more, as against most respondents in earlier surveys being overly optimistic that this can be achieved in six months to a year.

57 percent of survey respondents feel they do not have adequate knowledge and appropriate visibility of sub-contractors engaged by their third-parties and a further 21 percent are unsure on their organization's level of understanding.

Impact of changing regulations is considered to be the greatest contributory factor to the increased perception of inherent risks (49 percent of respondents) followed by heightened levels of regulatory scrutiny (45 percent of respondents).

Inability to manage third party risks leads to financial, reputational and customer impact
Samples of select regulations
Regulators and Industry Associations have issued new guidance for Financial Institutions to identify, monitor and report risks

Regulatory Evolution

- **2011**
  - **BCBS**: Principles for the Sound Management of Operational Risk and Operational Risk
  - **EBA**: Guidelines on Internal Governance (GL 44)

- **2012**
  - **BaFin**: Update to MaRisk/MaComp

- **2013**
  - **FSB**: Guidance for More Effective Supervision of Risk Appetite and Risk Culture at Financial Institutions
  - **COSO**: Updated version of - Internal Control—Integrated Framework

- **2014**
  - **OCC**: Guidelines for risk governance
  - **BCBS**: Corporate governance principles
  - **BaFin**: Translation of MaRisk
  - **APRA**: Prudential Standard CPS 220 - Risk Management

Renewed Emphasis on Risk Governance

Since 2011, the regulators have issued significant guidelines on risk governance and internal controls.

In 2012, BaFin published a new version of MaComp and a revised version of MaRisk as the requirements for risk management have grown steadily since the start of the financial crisis.

OCC issued enforceable final guidelines that establish minimum standards for the design and implementation of a risk governance framework for large insured national banks, insured federal savings associations, and insured federal branches of foreign banks.

COSO revised its Internal control-Integrated Framework to help organizations design and implement internal control in light of many changes in business and operating environments since the issuance of the original Framework in 1992.

FSB has introduced principles for an effective risk appetite framework to enable financial institutions to adapt to the changing economic and regulatory environment in order to manage new types of risk.

---

Regulators, Governments and Industry Associations have issued new guidance for Supplier/third party/Third Party/Outsourcing to identify, monitor and report risks.

Sample of select regulations - India

Regulatory Evolution

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>IT Act: Initiation of regulations on Information Technology – 2000</td>
</tr>
<tr>
<td>2008</td>
<td>IRDA: Third Party Administrators Health Services</td>
</tr>
<tr>
<td>2008</td>
<td>IT Act: Information Technology Amendment Act 2008</td>
</tr>
<tr>
<td>2010</td>
<td>DOT: Department of Telecom : Amendment to Unified Access Service License Agreement for Security – 2010</td>
</tr>
<tr>
<td>2011</td>
<td>SEBI: Guidelines on Outsourcing of Activities by Intermediaries - 2011</td>
</tr>
<tr>
<td>2013</td>
<td>TRAI: Issues new guidelines on outsourcing especially in VAS</td>
</tr>
<tr>
<td>2013</td>
<td>GOI: Companies Act 2013 released</td>
</tr>
<tr>
<td>2013</td>
<td>Companies Act, 2013 refers to Board responsibilities for third party Management</td>
</tr>
</tbody>
</table>

Renewed Emphasis on Risk Governance

Since 2001, the regulators and Government have issued significant guidelines on risk governance and internal controls.

Different agencies – Regulators and Government have been issuing guidelines on Supplier, Third Party and outsourced third party risk management.

RBI, IRDA, DOT / TRAI issued enforceable final guidelines that establish minimum standards for the design and implementation of a risk governance framework.
RBI Guidelines for Outsourcing

Regulatory Evolution

So, what is the solution?
Challenges with evolving Third Party Relationship

The time chart below maps ‘risks and challenges’ over years of maturing relationship with supplier:

- This mapping is based on our experience from past engagements where we assisted global banks and financial institutions during process transition or post transition
- We have also noticed that almost all these 9 risk areas prevailed over the entire lifetime of relationship however the probability of occurrence and business impact varies from risk type

<table>
<thead>
<tr>
<th>Supplier Relationship Timeline - Illustrative</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Year 0</strong></td>
</tr>
<tr>
<td><strong>Year 1-3</strong></td>
</tr>
<tr>
<td><strong>Year 3-5</strong></td>
</tr>
<tr>
<td><strong>Later</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Strategic Risk</th>
<th>Risk of inappropriate outsourcing decisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputation Risk</td>
<td>Risk of negative public opinion due to Suppliers that do not meet service expectations of the Bank’s customers</td>
</tr>
<tr>
<td>Compliance / Legal Risk</td>
<td>Suppliers’ services are inconsistent with the law and / or Bank’s policies</td>
</tr>
<tr>
<td>Transaction / Operational Risk</td>
<td>Engagement with key personnel SLA / Metrics 4th Party Suppliers Decreasing Service Levels</td>
</tr>
<tr>
<td>Financial Stability Risk</td>
<td>Improper evaluation criteria Supplier’s inability to generate profit or to maintain capital necessary to support ongoing operations</td>
</tr>
<tr>
<td>Integrity of Data</td>
<td>Inaccuracy of automated information and associated management information systems</td>
</tr>
<tr>
<td>Confidentiality of Information</td>
<td>Intentional or inadvertent disclosure of information to unauthorized individuals</td>
</tr>
<tr>
<td>Business Continuity Risk</td>
<td>Risk associated with ineffectiveness of Suppliers’ business continuity programs; risk of inadequate contingency planning by the Bank</td>
</tr>
<tr>
<td>Contractual Risk</td>
<td>Risk that Supplier contract provisions may be incomplete or inadequate</td>
</tr>
</tbody>
</table>

© 2018 Deloitte Touche Tohmatsu India LLP.
TPRM assessment maturity

A mature risk management program includes addressing independent audit reports, periodically assessing the third party’s information security posture and continuously monitoring the information security posture of existing and new third parties.

Organizations often falter by focusing their energy on conducting third party cyber risk assessments vs. managing third party cyber risks that matter.
Typical challenges

As threats and regulatory scrutiny have increased, organizations have evolved their third party risk programs. However in managing these programs, they continue to face challenges.

- Cognizance at the center – clear line-of-sight into compliance with policies, standards, and processes, including the evaluation of the effectiveness of processes and tools
- An effective organizational structure with clear roles, accountability, and responsibility - at multiple levels
- An integrated view of risk across multiple risk areas e.g., compliance, privacy, operational risk, business continuity
- Consistent application of exit process and strategy when third party or a service is terminated
- Manage and track third party performance and contract compliance
- Oversight and escalation activities and relaying information to risk managers
- Experienced resources to conduct comprehensive analysis on specific areas of risks; and turnover
- Maintaining a consolidated inventory of third parties across business units and functions
- Conducting adequate due diligence on third parties with higher inherent risk
- Conducting due diligence processes that are integrated with overall third party lifecycle

Ownership and interactions

Risk coverage and exposure

Adherence to exit strategy

Due diligence process

Risk and performance monitoring

Third party inventory

Challenges & Opportunities

Ownership and interactions

Risk coverage and exposure

Adherence to exit strategy

Due diligence process

Risk and performance monitoring

Third party inventory

Challenges & Opportunities
What did we learn from our survey?

44 percent of respondents have now invested in a centralized in-house CoE for EERM while another 30 percent utilize a central shared services organization (whether fully insourced or with some elements outsourced).

A further 15 percent have established federated structures and 14 percent operate as a “hub-and-spoke” model where centralized elements of EERM are becoming more common-place.

44%

30%

15%

14%

Organizations that are integrated or optimized in managing their extended enterprise are now typically investing over US$3 million annually on EERM initiatives, managed by more than 50 FTEs.

Skills, bandwidth, and competence of talent engaged in EERM-related activities appears to be the most significant concern for respondents (45 percent), followed by the clarity of roles and responsibilities and EERM processes (41 percent in either case).
TPRM Assessment Framework

**Policy, Procedures, Standards and Guidelines**

**Data Sources (Company Internal Systems like SAP and so on)**

**New/Existing third parties**
- Third party Evaluation
- Third party Selection
- Contract & On-board
- Termination

**Third party Prioritization**
- Parameters / Third party Information
- Risk Engine
- Third party Profile
- Third party Coverage Model

**Review Type**
- Contract Risk & Compliance Review
- InfoSec Review ISO27001/2, PCI, etc.
- SLA / Performance Review
- Integrity & Regulatory review
- Incident Review – Forensics, Fraud, etc.

**Review Method**
- Self Assessment
- Onsite
- Remote
- Continuous Monitoring
- Hybrid

**Manage, Monitor & Remediate**

**Key Performance Indicators (KPI)**

**Reporting**
- CISO Team
- SRC
- Procurement
- Others

**Automation**
- Views
- Work Flow
- Data Repository
- Analytics and Reporting

**Third Party Risk Management Project Management Office (PMO)**
- Planning Management
- Document Management
- Risk Management
- Knowledge Management
- Financial Tracking & Reporting

- Adherence to Project Lifecycle
- Communication Management
- Quality Management
- Value Add

© 2018 Deloitte Touche Tohmatsu India LLP.
Does technology provide a silver bullet?
How can Technology help in TPRM?

Preventive controls → Automation of TPRM process → Usage of analytics
Technology Enablement

Automation and Analytics

TPRM Automation Platform

- Report on your third party risk profile
- Track third party performance
- Build third party risk questionnaires
- Assess third party viability and impact on risk
- Perform third party due diligence
- Chart trends and insights with smart analytics
- Store and retrieve evidence for each assessment
- Scale and integrate with flexible workflows
- Customize reports and dashboards as per stakeholder requirement
- Trigger based approval and review actions
- Manage assessment findings
- Drag-and-drop user interface

© 2018 Deloitte Touche Tohmatsu India LLP.
What are the other developments I need to be aware of?
Insights into the future – Can you take advantage of the trends?

Risk sensing – Continuous Monitoring

&

Risk Exchange utility
Risk Sensing – An enabler for continuous monitoring

The traditional solution of conducting risk and control assessments for overseeing third party compliance is cost/labour intensive and often limited to cyber risk.

Integrating risk sensing capabilities with traditional techniques can provide deep and timely insights to address potential problems before they turn into incidents.

### Capabilities

- Enhances a significant portion of the traditional due diligence process and enables persistent monitoring for indications and warnings across multiple risk domains
- Incorporates data analytics to identify and monitor emerging risks
- Provides a rapidly customizable framework to generate accurate, relevant data for further research
- Conducts research from the vantage point of a trusted advisor and leverages a wide range of proprietary databases and subscription services

### Benefits

- Reduced costs, time and efforts
- Comprehensive research across the third party landscape
- Improved accuracy, thoroughness and timeliness
- Enabled strategic and informed decision making

### Risk sensing applicability scenarios

1. **Pre-contract due diligence**
   - Apply risk sensing rather than a customized risk assessment due to time and resource constraints
   - Identifies major issues or concerns before entering into a contractual agreement

2. **Low risk oversight**
   - Apply risk sensing on low risk third parties as part of ongoing monitoring activities
   - Alleviates resource constraints and allows focus on third parties that pose a higher risk to the organization

3. **Prioritized risk management**
   - Apply risk sensing on all third parties as part of ongoing monitoring activities
   - Risk scores will help determine which third parties require more comprehensive analysis on specific areas of risk

There are several other similar solutions in the market – RiskIQ, Security Scorecard
Risk Sensing Approach
Risk-control monitoring framework for third party

1. Plan (Define & Update)
- Identify third party risks based on
  - Legal and regulatory requirements
  - Industry leading practices and standards
- Define / update KRIs for third party risks
- Communicate the KRIs and reporting process to relevant stakeholders based on applicability

4. Review & Manage
- Review the KRI dashboard for third party risks
- The information in KRI dashboard will assist in making decisions pertaining to third party risk management

2. Monitor & Assess
- third party report status of the risks with relevant evidences at a defined frequency
- Assess the risks based on the evidences shared by the third party
- Update the value of applicable KRIs for each third party

3. Analyze & Report
- Update the KRI dashboard for all third party
- Publish the KRI dashboard to relevant stakeholders at a defined frequency
The Emerging Trend – Sharing Cost and Value Across Organizations. A community model, like an Exchange, helps enterprises and third parties mobilize around a standardized and dynamic set of TPRM data, while leveraging a shared cost model and the collective benefits of each others actions.

The chart illustrates how members benefit from a community model based on multiple participants

**Standardize, streamline**

**Improve insights**

**Reduce costs**

**Increase accountability**

**Third Party Risk Utility Exchange: The Most Cost-Effective Approach**

Always know which third parties pose the most risk to your enterprise. spot cyber risk sooner and respond to threats from third parties faster
Transforming third party cyber risk management

Standardize, streamline

**Simplified, streamlined, and industry-standard assessment content**
- Industry leading practices and regulatory requirements
- Mapped to industry standards (e.g., NIST, HIPAA, ISO27001)

Reduce costs

**Cost-efficient, timely, and low overhead execution**
- Fewer internal resources required
- Lower cost to do business
- Global skills when you need them

Increase accountability

**Business and third-party alike**
- Near-time and on-demand access
- Quicker turnaround with dedicated and trained professionals
- Stronger business and third-party relationships
- Cost-mutualization

Improve insights

**Structured data, advanced analytics and ongoing monitoring**
- Relationship risk management vs. data gathering
- Actionable data before contracting completion
- Enterprise reporting and trend analysis

We can help organizations quickly enhance their third-party programs, create efficiencies, and build confidence in their third-party risk posture in order to realize a host of benefits
Key contacts

Munjal Kamdar  
Partner  
CISSP, ISO 27001 LA

Sharda Rokde  
Senior Manager  
CIPP, ISO 27001 LA
Annexure

- https://www.bis.org/list/bcbs/tid_28/index.htm
- https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Meldung/2014/meldung_140815_marisk_uebersetzung_en.html
- http://meity.gov.in/content/information-technology-act
- https://www.irdai.gov.in/ADMINCMS/cms frmGeneral_NoYearList.aspx?DF=RL&mid=3.2.1
- https://www.india.gov.in/access-services-department-telecommunications
- https://www.iso.org/standard/54534.html
- https://rbidocs.rbi.org.in/rdocs/notification/PDFs/LBS300411F.pdf