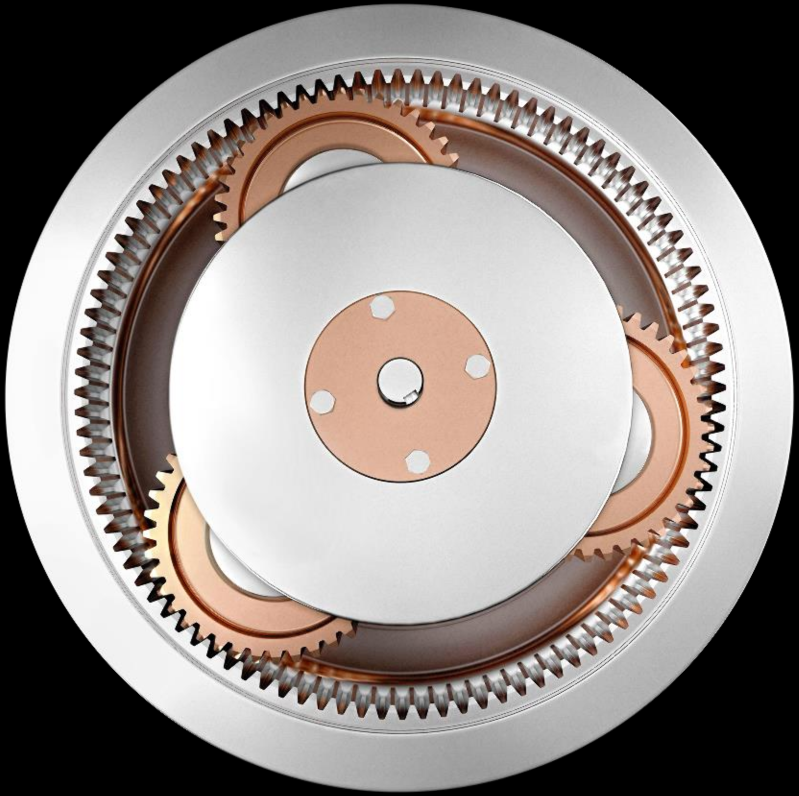
Deloitte.



# Point of View - Third Party Risk Management

**Deloitte Touche Tohmatsu India LLP**

May 2018

Risk Advisory

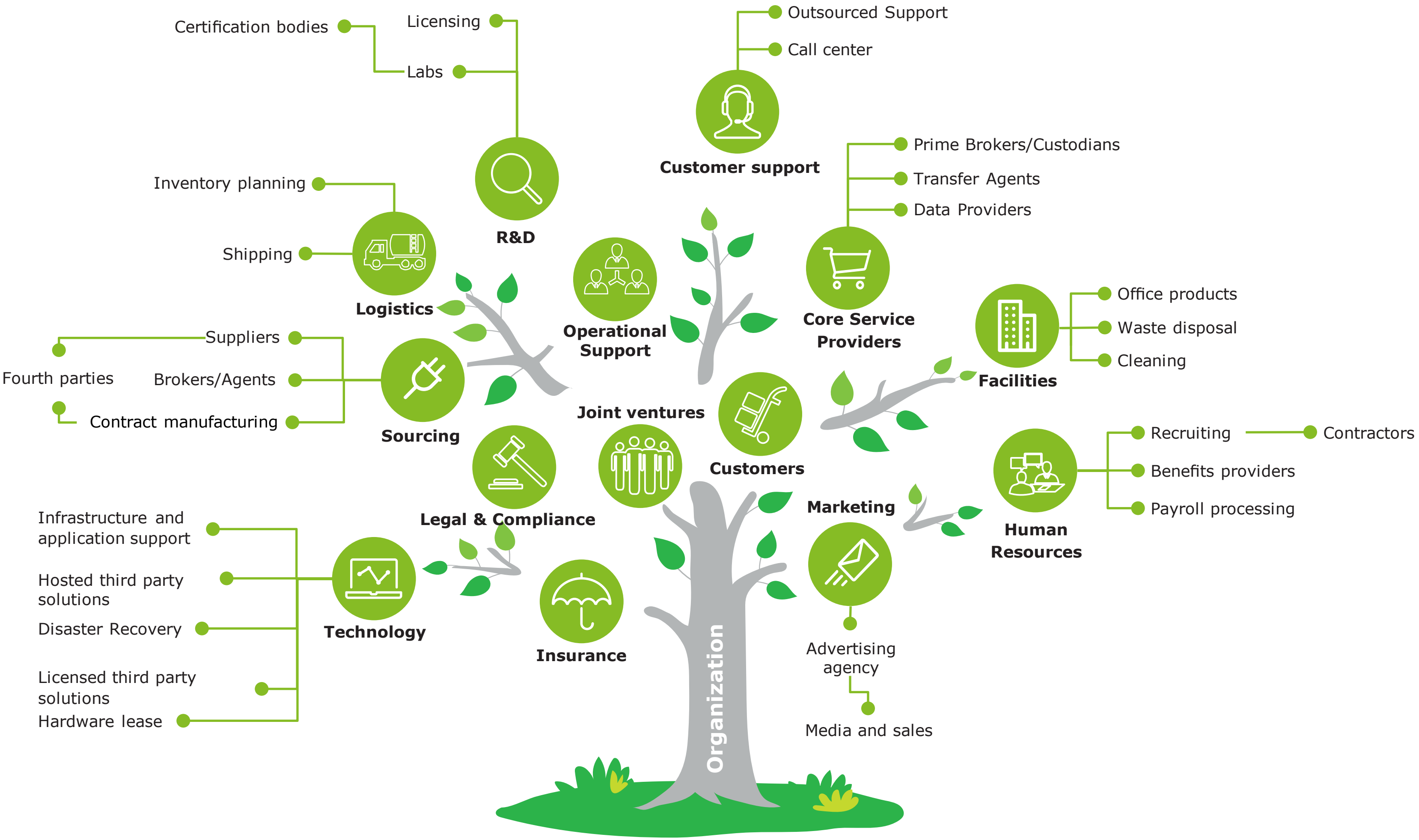
# How will you get ROI on your time investment today?

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….

## Drivers and Stakeholders

| Third party Vulnerability | Contract Compliance | Regulatory Compliance | Dispute | Performance Management | Reputation Management |
|---|---|---|---|---|---|

## Scope of Assurance

| Solvency | Security | Regulatory | Corporate Responsibility | Resiliency | Health Safety and Environment | Intellectual Property | Billing and Performance | Integrity |
|---|---|---|---|---|---|---|---|---|
| • Financial performance<br>• Liquidity<br>• Profitability<br>• Funding | • Information Security<br>• Data Security<br>• Data Privacy<br>• Physical Security | • Competition<br>• Data Protection<br>• Market Specific Privacy | • Sustainability<br>• Labor<br>• Working conditions<br>• Human Rights<br>• Quality | • Continuity<br>• Data Recovery<br>• Product recall | • Environment<br>• Hazardous materials<br>• Health and Safety | • Identification<br>• Protection<br>• Development<br>• Research<br>• Licensing | • Measurement<br>• Service delivery<br>• Financial Compliance | • Anti-bribery conflicts<br>• Interdependence<br>• Ethics<br>• Fraud |

## Monitoring and Reporting

## Approach and Methodology

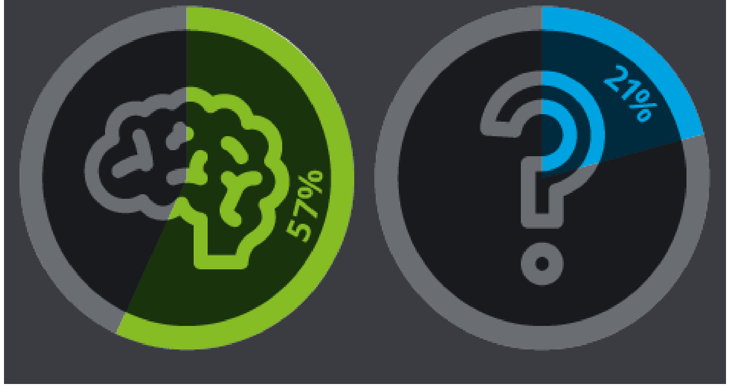
| Self Assessment | Industry Standards | Corporate Standards | Controls Assurance | Shared Assessments | Certification | Post incident |
|---|---|---|---|---|---|---|

# CxO speak – Why is it a Boardroom / Regulator conversation?

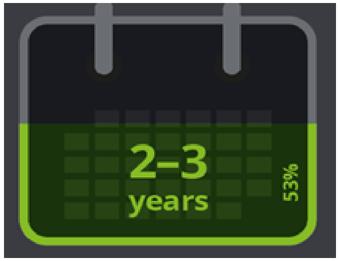
# Why do organization need third party risk management capabilities?

**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.

**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.



**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.



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)

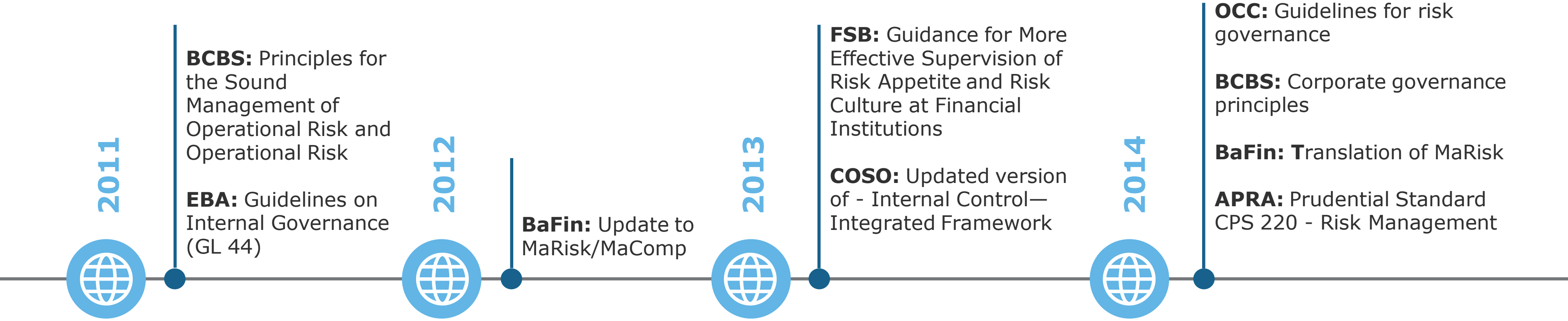
**Inability to manage third party risks leads to financial, reputational and customer impact**

The Deloitte TPRM/EERM 2018 survey statistics

# 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: T**ranslation 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[1]

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[2]

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[3]

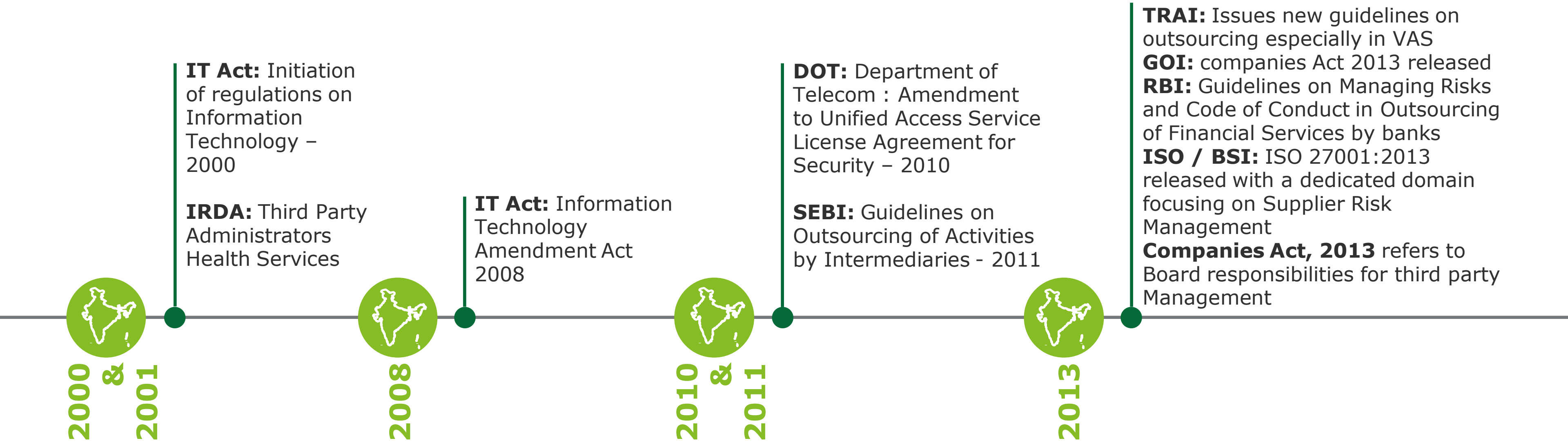
FSB has introduced principles for an effective risk appetite framework to enable financial institutions to adapt to the changing economic and regulatory environment in order to manage new types of risk[4]

[1] BaFin Annual Report 2012; [2] OCC Bulletin 2014-45; [3] COSO Internal Control — Integrated Framework (2013); [4] FSB Principles for an Effective Risk Appetite Framework

# Sample of select regulations - India

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

## Regulatory Evolution



2000 & 2001

**IT Act:** Initiation of regulations on Information Technology – 2000

**IRDA:** Third Party Administrators Health Services

2008

**IT Act:** Information Technology Amendment Act 2008

2010 & 2011

**DOT:** Department of Telecom : Amendment to Unified Access Service License Agreement for Security – 2010

**SEBI:** Guidelines on Outsourcing of Activities by Intermediaries - 2011

2013

**TRAI:** Issues new guidelines on outsourcing especially in VAS
**GOI:** companies Act 2013 released
**RBI:** Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks
**ISO / BSI:** ISO 27001:2013 released with a dedicated domain focusing on Supplier Risk Management
**Companies Act, 2013** refers to Board responsibilities for third party Management

### Renewed Emphasis on Risk Governance

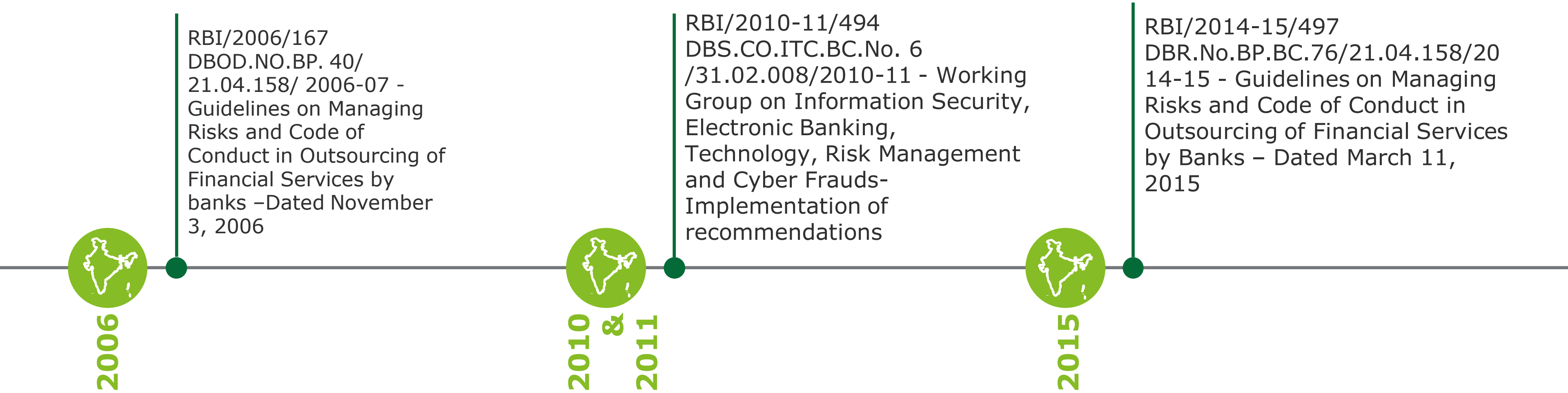
Since 2001, the regulators and Government have issued significant guidelines on risk governance and internal controls

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



2006

RBI/2006/167 DBOD.NO.BP. 40/ 21.04.158/ 2006-07 - Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks –Dated November 3, 2006

2010 & 2011

RBI/2010-11/494 DBS.CO.ITC.BC.No. 6 /31.02.008/2010-11 - Working Group on Information Security, Electronic Banking, Technology, Risk Management and Cyber Frauds- Implementation of recommendations

2015

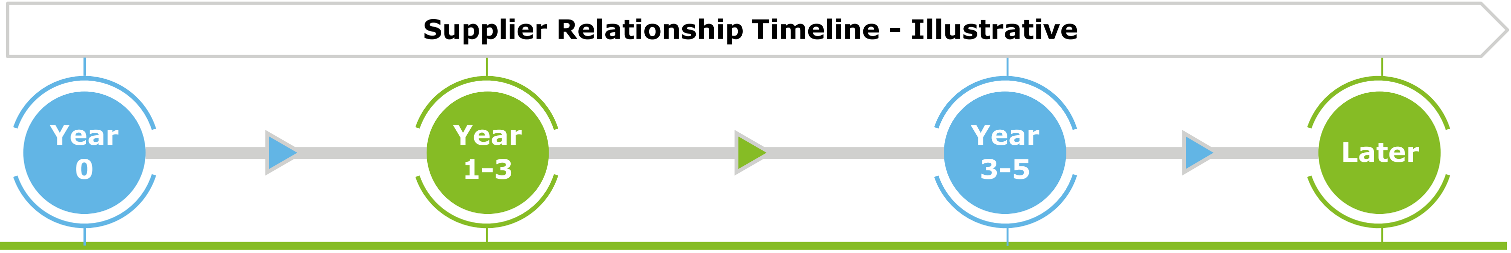
RBI/2014-15/497 DBR.No.BP.BC.76/21.04.158/2014-15 - Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks – Dated March 11, 2015

# 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:**

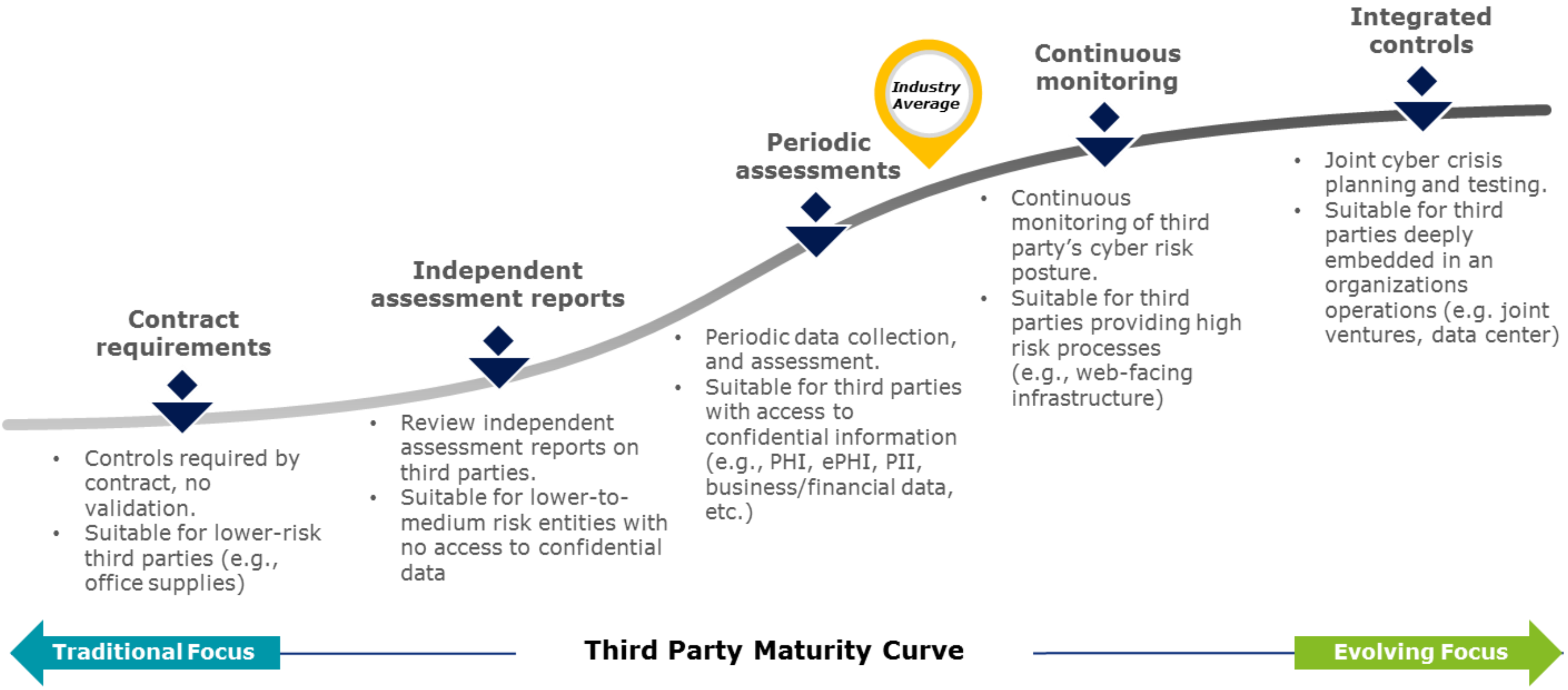
- This mapping is based on our experience from past engagements where we assisted global banks and financial institutions during process transition or post transition
- We have also noticed that almost all these 9 risk areas prevailed over the entire lifetime of relationship however the probability of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



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

# 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



**Contract requirements**

- Controls required by contract, no validation.
- Suitable for lower-risk third parties (e.g., office supplies)

**Independent assessment reports**

- Review independent assessment reports on third parties.
- Suitable for lower-to-medium risk entities with no access to confidential data

**Periodic assessments**

- Periodic data collection, and assessment.
- Suitable for third parties with access to confidential information (e.g., PHI, ePHI, PII, business/financial data, etc.)

**Continuous monitoring**

- Continuous monitoring of third party's cyber risk posture.
- Suitable for third parties providing high risk processes (e.g., web-facing infrastructure)

**Integrated controls**

- Joint cyber crisis planning and testing.
- Suitable for third parties deeply embedded in an organizations operations (e.g. joint ventures, data center)

**Traditional Focus** — **Third Party Maturity Curve** — **Evolving Focus**

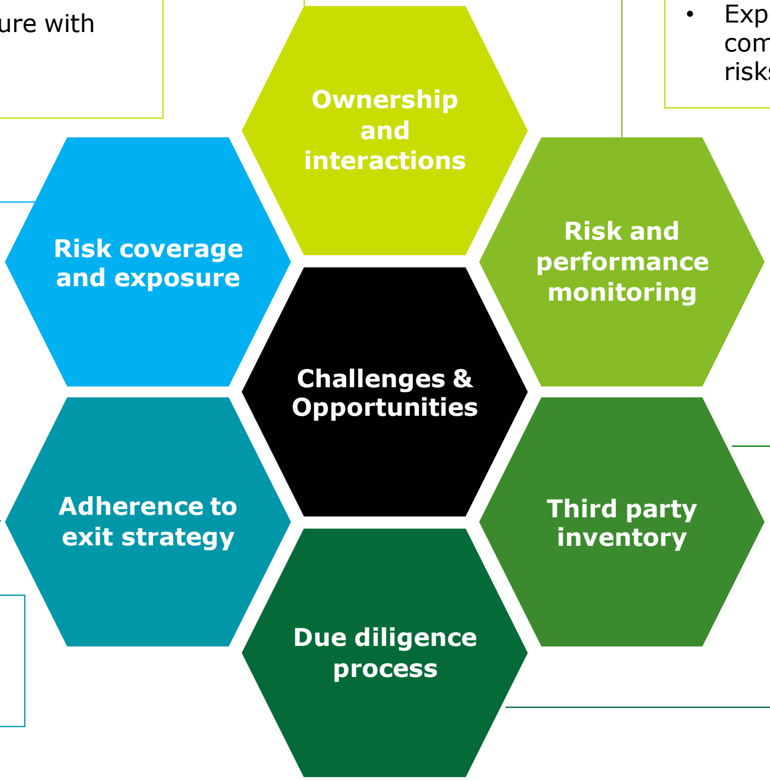
Organizations often falter by focusing their energy on conducting third party cyber risk assessments vs. managing third party cyber risks that matter.

# 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

- 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


Ownership and interactions
Risk coverage and exposure
Risk and performance monitoring
Challenges & Opportunities
Adherence to exit strategy
Third party inventory
Due diligence process

- An integrated view of risk across multiple risk areas e.g., compliance, privacy, operational risk, business continuity

- Maintaining a consolidated inventory of third parties across business units and functions

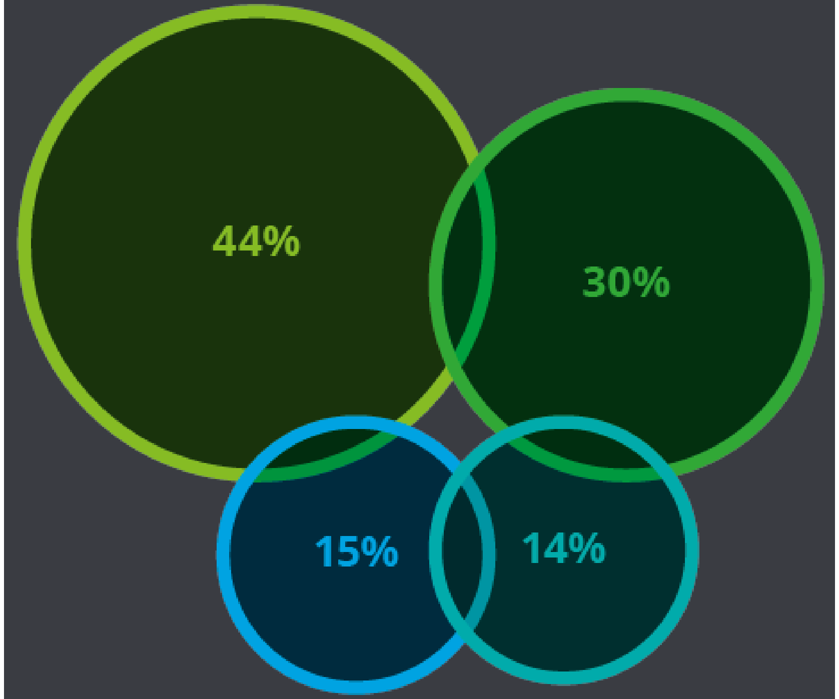
- Consistent application of exit process and strategy when third party or a service is terminated

- Conducting adequate due diligence on third parties with higher inherent risk
- Conducting due diligence processes that are integrated with overall third party lifecycle

# 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).

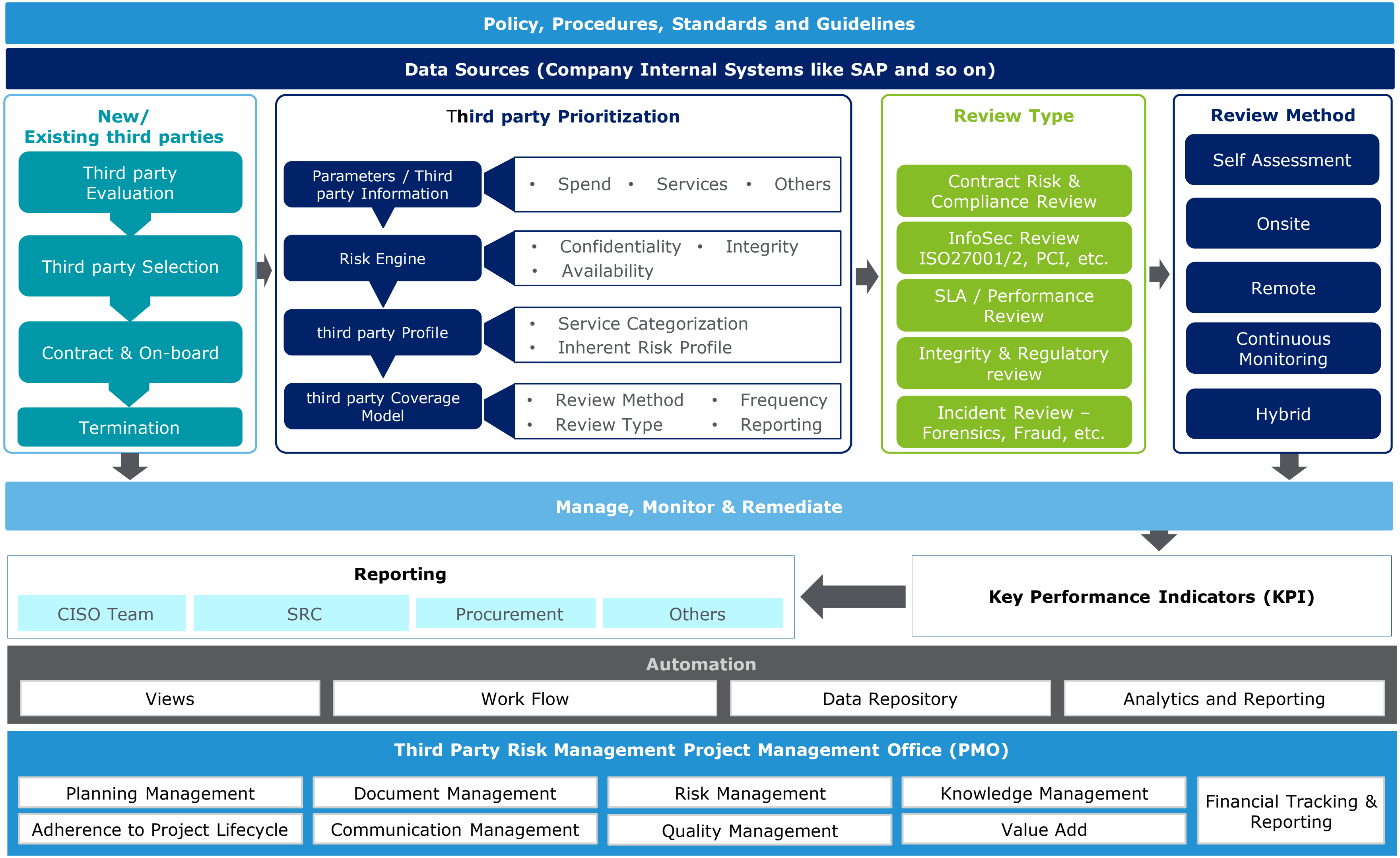
A further **15 percent** have established federated structures and **14 percent** operate as a "hub-and-spoke" model[6] where centralized elements of EERM are becoming more common-place.



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
  - Spend
  - Services
  - Others
- Risk Engine
  - Confidentiality
  - Integrity
  - Availability
- third party Profile
  - Service Categorization
  - Inherent Risk Profile
- third party Coverage Model
  - Review Method
  - Frequency
  - Review Type
  - Reporting

**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**

**Reporting**

- CISO Team
- SRC
- Procurement
- Others

**Key Performance Indicators (KPI)**

**Automation**

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

**Third Party Risk Management Project Management Office (PMO)**

- Planning Management
- Adherence to Project Lifecycle
- Document Management
- Communication Management
- Risk Management
- Quality Management
- Knowledge Management
- Value Add
- Financial Tracking & Reporting

# Does technology provide a silver bullet?

# How can Technology help in TPRM?

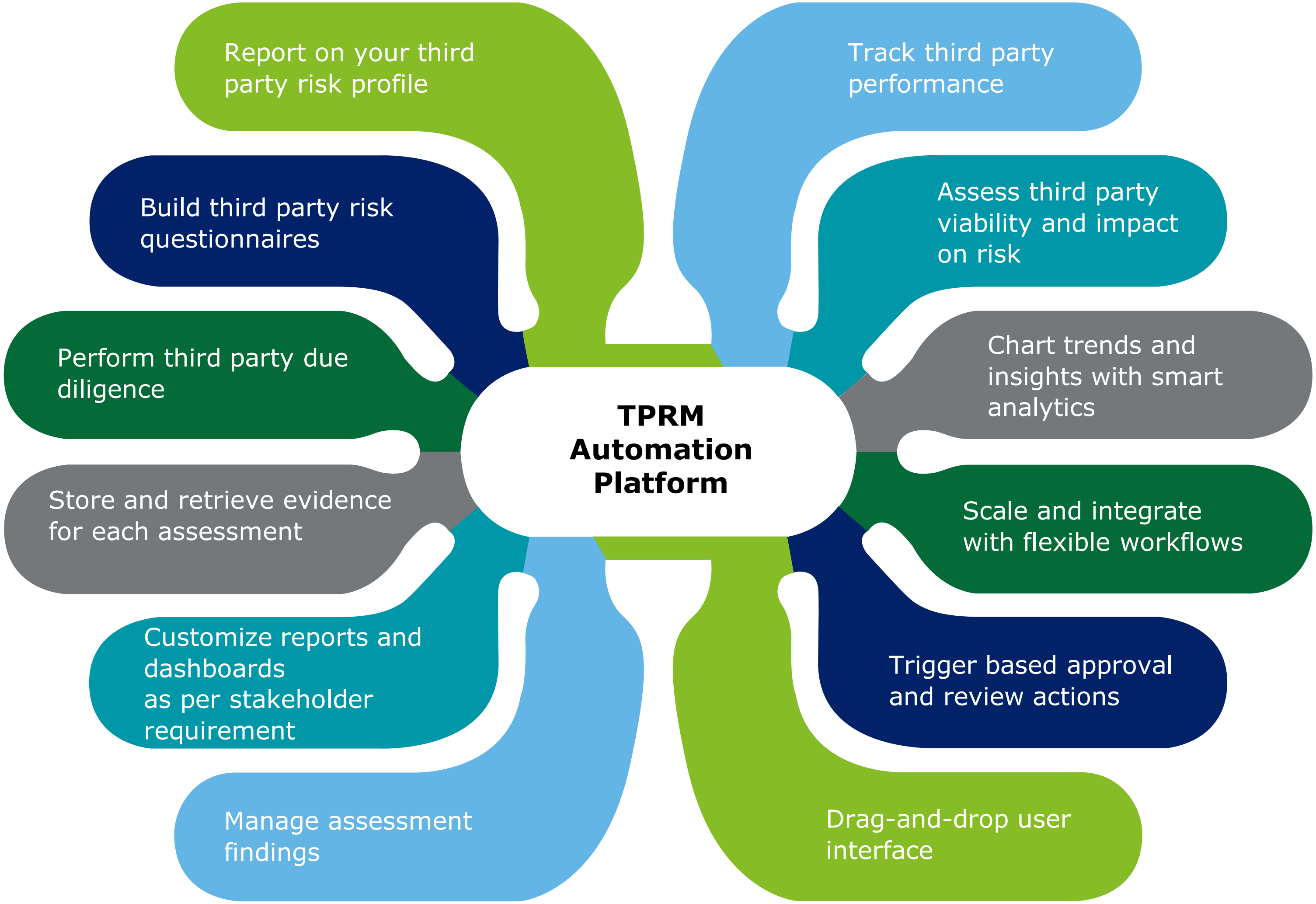
**Preventive controls**

**Automation of TPRM process**

**Usage of analytics**

# Technology Enablement

## Automation and Analytics



TPRM Automation Platform

Report on your third party risk profile

Build third party risk questionnaires

Perform third party due diligence

Store and retrieve evidence for each assessment

Customize reports and dashboards as per stakeholder requirement

Manage assessment findings

Track third party performance

Assess third party viability and impact on risk

Chart trends and insights with smart analytics

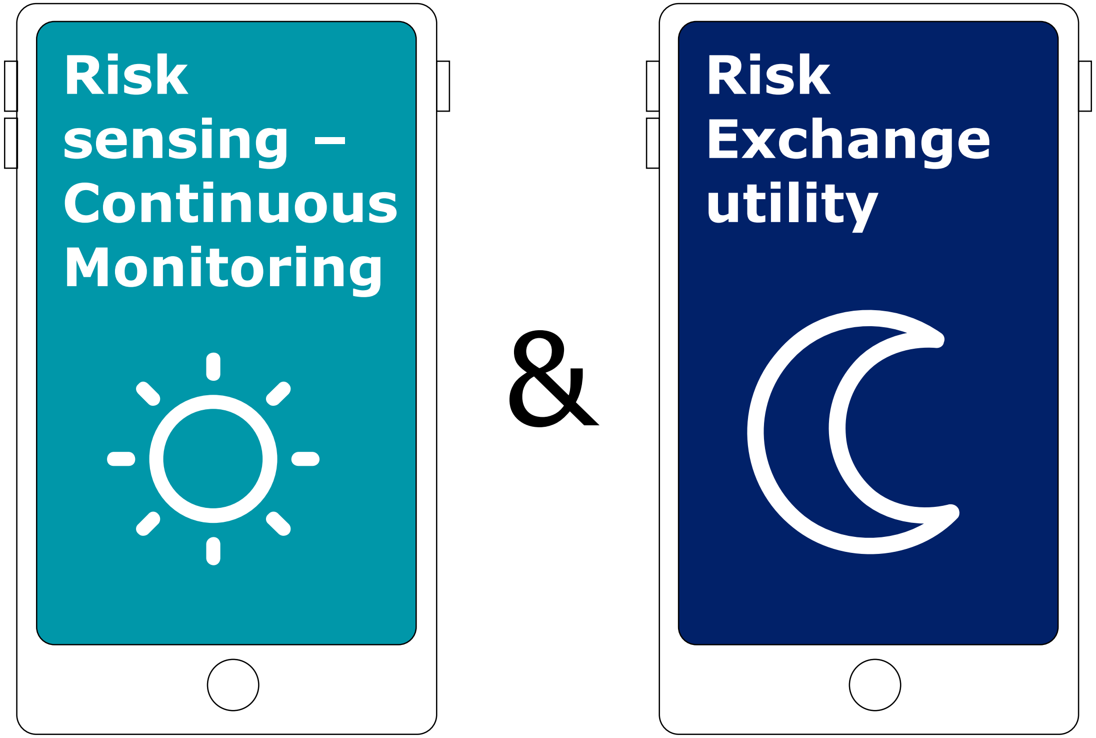
Scale and integrate with flexible workflows

Trigger based approval and review actions

Drag-and-drop user interface

# What are the other developments I need to be aware of?

# Insights into the future – Can you take advantage of the trends?



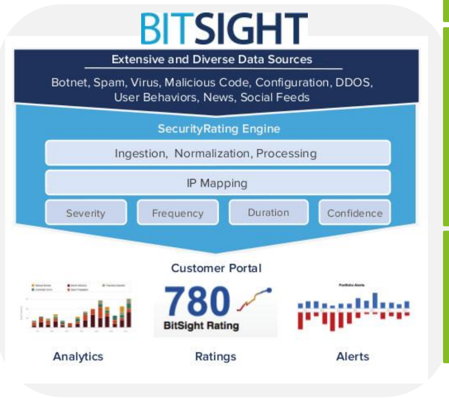
Risk sensing – Continuous Monitoring

&

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.


BITSIGHT
Extensive and Diverse Data Sources
Botnet, Spam, Virus, Malicious Code, Configuration, DDOS, User Behaviors, News, Social Feeds
SecurityRating Engine
Ingestion, Normalization, Processing
IP Mapping
Severity
Frequency
Duration
Confidence
Customer Portal
780
BitSight Rating
Analytics
Ratings
Alerts

**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

### 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

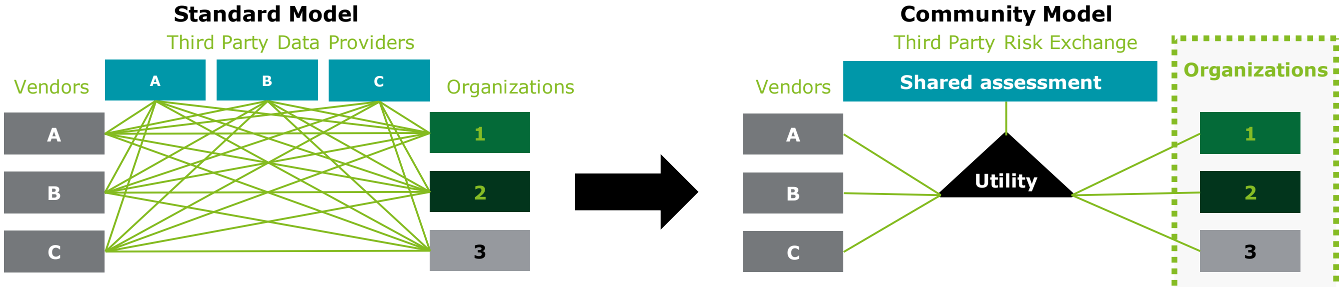
- Update the KRI dashboard for all third party
- Publish the KRI dashboard to relevant stakeholders at a defined frequency

### 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

# Risk Exchange Utility– Redefining the approach

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

Effective third-party management

## 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.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-
- https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2017/fa_bj_1711_MaRisk_en.html
- http://www.fsb.org/2013/11/r_131118/
- https://www.coso.org/documents/COSO%20McNallyTransition%20Article-Final%20COSO%20Version%20Proof_5-31-13.pdf
- https://www.occ.gov/publications/publications-by-type/comptrollers-handbook/corporate-risk-governance/pub-ch-corporate-risk.pdf
- https://www.coso.org/documents/COSO%20McNallyTransition%20Article-Final%20COSO%20Version%20Proof_5-31-13.pdf
- https://www.occ.gov/publications/publications-by-type/comptrollers-handbook/corporate-risk-governance/pub-ch-corporate-risk.pdf
- https://www.iif.com/news/revised-corporate-governance-principles-banks-consultation-paper-issued-basel-committee
- https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Meldung/2014/meldung_140815_marisk_uebersetzung_en.html
- https://www.legislation.gov.au/Details/F2014L01640/Explanatory%20Statement/Text
- https://en.m.wikipedia.org/wiki/Information_Technology_Act,_2000
- 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://taxguru.in/rbi/guidelines-managing-risks-code-conduct-outsourcing-financial-services-banks.html
- https://www.iso.org/standard/54534.html
- https://mca.gov.in/Ministry/pdf/CompaniesAct2013.pdf
- https://www.rbi.org.in/commonman/Upload/English/Notification/PDFs/73713.pdf
- https://rbidocs.rbi.org.in/rdocs/notification/PDFs/LBS300411F.pdf
- https://www.rbi.org.in/SCRIPTS/BS_PressReleaseDisplay.aspx?prid=33673

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see **www.deloitte.com/about** for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.