Be responsible and effective:
Strike a balance
ISACA New Delhi Chapter (31-October-2020)
Speakers: Vikas Garg (Director – Deloitte) & Gunjan Mody (Associate Director – Deloitte)
Contents

1. What is Extended Enterprise?
2. Importance of EERM
3. Governing and Operationalizing EERM
4. 2020 Deloitte Global TPRM survey
5. What You should Expect Next
What is your Extended Enterprise?

The extended enterprise is the concept that an organisation does not operate in isolation. Its success is dependent upon a complex network of third party relationships.
Why Is Extended Enterprise Risk Management (EERM) Important?

Deloitte’s annual global surveys on EERM confirm that incidents and risks related to the extended enterprise are on the rise, as organizations struggle with several challenges.

**Key risks and challenges**

- Demand for cost & process efficiencies, leading to incidents
- Limited visibility into sub-contractor relationship
- Inability to determine third-party compliance
- Lack of confidence or transparency into third-party operations
- Inherent risk & maturity concerns
- Compatibility issues among varied technology platforms
- Lack of a centralized control mechanism

- **83%** of organizations experienced a third party incident in the past three years
- **50%** of organizations do not understand the nature of individual third party relationships
- **41%** of organizations do not monitor third parties based on their risk profile
- **49%** of respondents feel that impact of changing regulations is considered to be the greatest contributory factor
- **28%** of organizations do not identify, assess or monitor subcontractors at all or assess only at the time of onboarding a new third party
**Impact from Extended Enterprise Risks and Incidents**

1. **Loss of reputation** - Risk to the reputation of the organization from the use of third party relationships due to a myriad of reasons including misuse of intellectual property; poor product quality; lack of compliance to human rights and environmental regulations, etc.

2. **Supply chain disruption** - Key third party business disruption due to bankruptcy, geo political issues, macro risks etc. can result in supply chain disruption

3. **Data risk** - Loss, misuse or mishandling of critical data of the organization or its customers by a third party relationship can result in financial loss; hefty fines and decrease in shareholder value

4. **Product recall** - Poor product quality, safety issues or faulty packaging by third parties can lead to product recalls resulting in recall costs, lawsuits from consumers, increased costs from settlements, and lost revenue from missed sales opportunities

5. **Financial impact** - Financial loss from under-reporting of revenue from licensees, royalty partners, distributors, franchisees etc. and over-payments for services from third party relationships

6. **Lack of compliance** - Third party acts corruptly to gain business advantage for organization, or making organization non-compliant to regulations including Environment, Health and Safety, Labor Rights etc., resulting in hefty fines

7. **Poor Performance** - Lack of sustained performance from third party relationships resulting in costly mistakes, over allocation of capital to relationship and defeating the purpose of outsourcing strategy
Governing the Extended Enterprise

**Govern**

Strategic management exists to ensure a single view of extended enterprise risk to the organization. Well-defined roles and responsibilities to manage the extended enterprise lifecycle and integration points with other functions.

**Manage**

Formal processes exist to assess the effectiveness of the EERM program against EERM framework. Policies, standards & procedures defining EERM methodology and activities, risk tolerance levels.

**Operate**

Coordinated communication channel to inform and educate relevant stakeholders. Tools and technology to manage large extended enterprise landscape and ensure compliance to organization EERM framework.

Formal contracts management process is in place. Metrics and reporting for continuous monitoring and improvement of the extended enterprise control environment.
# Maturity Model

<table>
<thead>
<tr>
<th>Stage</th>
<th>Maturity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adhoc</td>
<td>Strategy</td>
<td>Strategy exists in isolated circumstances. Governance process and framework not explicitly defined.</td>
</tr>
<tr>
<td></td>
<td>Governance</td>
<td>Exclusively ad-hoc with no oversight or standard. Governance process and framework defined but needs revision and effective implementation.</td>
</tr>
<tr>
<td></td>
<td>Policies, Standards &amp; Procedures</td>
<td>Acceptance &amp; Standard defined but not implemented. Governance framework and processes are clearly defined, but implementation is limited.</td>
</tr>
<tr>
<td></td>
<td>Communication, Training &amp; Awareness</td>
<td>Defined &amp; agreed upon Integration with other processes is evolving. Governance framework and processes are clearly defined, effectively implemented, but no process improvements.</td>
</tr>
<tr>
<td></td>
<td>Risk Management Process</td>
<td>Defined &amp; agreed upon. Governance framework and processes are clearly defined, effectively implemented, and regularly enhanced for changes.</td>
</tr>
<tr>
<td></td>
<td>Contracts</td>
<td>Defined &amp; agreed upon. Governance framework and processes are clearly defined, effectively implemented, and regularly enhanced.</td>
</tr>
<tr>
<td></td>
<td>Technology &amp; tools</td>
<td>Defined &amp; agreed upon. Governance framework and processes are clearly defined, effectively implemented, and regularly enhanced.</td>
</tr>
<tr>
<td></td>
<td>Metrics &amp; reporting</td>
<td>Defined &amp; agreed upon. Governance framework and processes are clearly defined, effectively implemented, and regularly enhanced.</td>
</tr>
<tr>
<td></td>
<td>Measured</td>
<td>Defined &amp; agreed upon. Governance framework and processes are clearly defined, effectively implemented, and regularly enhanced.</td>
</tr>
<tr>
<td></td>
<td>Optimized</td>
<td>Defined &amp; agreed upon. Governance framework and processes are clearly defined, effectively implemented, and regularly enhanced.</td>
</tr>
</tbody>
</table>

## Key Terms

- **Adhoc**: Strategy exists in isolated circumstances. Governance process and framework not explicitly defined.
- **Repeatable**: Exclusively ad-hoc with no oversight or standard. Governance process and framework defined but needs revision and effective implementation.
- **Defined**: Acceptance & Standard defined but not implemented. Governance framework and processes are clearly defined, but implementation is limited.
- **Measured**: Defined & agreed upon Integration with other processes is evolving. Governance framework and processes are clearly defined, effectively implemented, but no process improvements.
- **Optimized**: Defined & agreed upon. Governance framework and processes are clearly defined, effectively implemented, and regularly enhanced for changes.

## Additional Notes

- **Strategy**
  - No risk management process and risks are looked after after an incident.
  - Limited third party contractual agreements exist or are measured.
  - Clearly inadequate tools are utilized for third party tracking.
- **Governance**
  - Adhoc communication and trainings when required.
  - Repeatable procedures exist without standards or enterprise-wide acceptance.
  - Communication & Training processes defined but need major revision.
- **Policies, Standards & Procedures**
  - Adhoc communication and trainings when required.
  - Communication & Training processes defined but need major revision.
  - Communication & Training processes are well clearly defined, but not implemented.
- **Risk Management Process**
  - Processes are clearly defined, effectively implemented, but no process improvements.
  - Standards for third party contracts in place but awaiting adoption.
- **Contracts**
  - A clear risk management process is defined and effectively implemented, but not updated as per changes in objectives.
  - Standards for info data elements do exist, but without integration to other IT processes and lacks automation.
- **Technology & tools**
  - Underpinned contracts including tracking monitoring.
  - Accepted ITSM tool used to track all third party info, includes Contracts, performance vs. SLAs.
- **Metrics & reporting**
  - Consistent standards exist to ensure compliance with agreed upon service levels.
How to operationalize EERM?

Policy, Procedures, Standards and Guidelines

Data Sources (Company Internal Systems like ERP, CRM, Billing System)

Third party Profiling & Prioritization

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

Third parties Lifecycle

- Third party Evaluation
- Third party Selection
- Contract & On-board
- Termination

Third party Profiling & Prioritization

- Spend
- Services
- Others
- Confidentiality
- Integrity
- Availability
- Service Categorization
- Inherent Risk Profile
- Review Method
- Frequency
- Review Type
- Reporting
- Review of business controls
- Review of both business and information security controls
- Review of information security controls

Domains

- Financial Health /Solvency
- Contract Risk & Compliance
- Information Security & Cyber Security
- Privacy Review
- Health & Safety
- SLA / Performance Review
- Integrity & Regulatory review
- Quality review
- Employment Practices

Review Method

- Self Assessment
- Onsite
- Remote
- Hybrid

Manage, Monitor & RemEDIATE

CISO Team
Chief Risk Office
Supply chain
Business Controller

Key Performance Indicators (KPI)

Enablers - Automation

- Dashboards
- Work Flow
- Data Repository
- Analytics and Reporting
Deloitte’s Third-party risk management (TPRM) Global survey 2020

Number of respondents (2016-2020)

- **2020**: 1,145 responses
- **2019**: 1,055 responses
- **2018**: 975 responses
- **2017**: 536 responses
- **2016**: 173 responses

**Cost of failure**
The financial impact of a failure by a third party or subcontractor has at least doubled over the past five years, according to almost half of respondents.

**Balancing responsibility and cost**
The desire to be socially responsible business has become one of the top drivers of investment in EERM.

**Increasing regulatory activity**
A rise in regulatory activity encourages nimble organizations to progress towards a greater EERM maturity.

**Leveraging external assistance**
A growing number of organizations use external support - risk intelligence, utility models, and managed services to supplement EERM program.

**Wider focus**
Senior executives are extending their focus beyond risk to include a broader view of third-party management.

**Vision for transformation**
Many organizations are developing longer-term visions of EERM transformation for coming 2 or 3 years.
Cost of failure
The financial impact of a failure by a third-party or subcontractor has at least doubled over the past five years, according to almost half (46%) of respondents. One in five believe the financial impact has multiplied tenfold.

84% of organizations experienced a third-party incident in the last three years, slightly up from 83% last year. 17% organizations faced a **high-impact** third-party risk incident which is sharply up compared to last year 11%.

A further 26% estimated this share price fall between 5% and 10%.

30% of listed companies surveyed believe **share prices could fall by 10% or more after an incident**, if third-party risks are not adequately managed.

- **2015**
  - US$ 2.50 million
  - 0%

- **2020**
  - US$ 50 million - US$1 billion
  - 19%
  - 11%
  - 84%
  - 17%

- **2020**
  - US$500 million or more
  - 30%
Balancing responsibility and cost
The desire to be a responsible business has become one of the top drivers of investment in EERM.

For the first time in the past five years, being a responsible business, and building a reputation for being one, is a top motivation for EERM investment.

Top EERM investment drivers

1. Response to 3rd party incidents 47%
2. Regulatory scrutiny 45%
3. Responsible business 43%
4. Cot reduction 39%

Contrary to the drivers following proportion of respondents do not allocate budget to risk domains impacting responsible and ethical business behaviour:

- Labour and modern slavery risk 54%
- Environmental risk (air pollution, water waste) 57%
- Climate risk 74%
EERM investment remains skewed towards certain risk domains

Budget for managing third-party risk is more likely to be allocated across a greater number of risk domains than last year, however, investment is still skewed towards:

- Information security: 65%
- Cyber risk: 60%
- Data privacy: 60%
- Health and safety: 57%
- Anti-bribery and corruption: 55%
- Regulatory non-compliance: 55%

This is not surprising given the largest third-party risks are considered as:

- Information security: 23%
- Cyber risk: 13%
- Anti-bribery and corruption: 10%

And the largest proportion of third-party incidents were related to:

- Information security: 9%
- Cyber risk: 11%
- Anti-bribery and corruption: 10%

These risk domains are also more universally applicable to organizations across industry sectors and have been the focus of regulatory attention over the last few years.
Budget is not prioritized, and organizations potentially risk underinvesting, in the following risk domains:

- **Subcontractor risk**: 32%
- **Climate risk**: 26%
- **Concentration risk**: 31%
- **Geopolitical risk**: 26%

Less than half organizations allocated budget to third-party business continuity. Many organizations have only initiated business continuity planning with their third parties as they respond to COVID-19.

- **59%** of respondents still believe they are under-investing in EERM, although this is quite a considerable fall from 70% last year.
- **58%** think budgets for managing third-party risk are inadequate.
Increasing regulatory activity
A rise in regulatory activity encourages nimble organizations to progress towards a greater EERM maturity. Those unable to keep pace with changing expectations fall behind their peers on the maturity journey.

Nearly half of respondents have stepped up their investments in EERM due to tightening pressure from regulators.

What’s impeding EERM maturity?

EERM maturity is impeded because many organizations do not cover or consider all third-party relationship types in their programs.

- Licensees and joint venture partners: 20%
- Sales agents, distributors and franchisees: 19%
- Group companies, subsidiaries and affiliates: 15%
- Only 15% of organizations consider themselves to be integrated or optimized
- 3/4 of respondents are either in defined or managed state
- 2% of organizations consider themselves to be integrated or optimized

45%
Management of subcontractor relationships at various levels and the management of smaller third-party relationships remain key challenges in relation to regulatory goalposts.

Only 20% of respondents say they can effectively monitor either all or even just the more critical subcontractors.

- 23% do not monitor subcontractors at all, even through third parties
- 29% rely solely on third parties for subcontractor management
- 15% identify and review subcontractors on an ad hoc basis
- 13% review subcontractors at the initiation of any new contract with a third-party
- Only 8% of organizations regularly identify and monitor all subcontractors...
- Though another 12% do monitor subcontractors of critical third parties

59% of respondents believe their EERM procedures are not flexible enough to proportionately and suitably assess smaller third parties, such as start-ups, sole traders, and the contingent workforce.
Vision for transformation
Organizations are developing longer-term visions of EERM transformation for the coming two or three years. This involves holistic rather than piecemeal management of third parties, enabled by a “single source of the truth”: a centralized repository of intelligence built on cutting edge technology.

Organizations are not satisfied with their EERM technology

- 24% are dissatisfied
- 48% are partly dissatisfied

Respondents biggest technology concern is that EERM systems do not seamlessly integrate with each other

- 34% say their technology’s reporting capability is inadequate for making critical business decisions about third parties
- 32% say the data’s integrity is questionable

- 61% of organisations

Want to explore a different technology solution

- 39% want to explore a different technology solution

Are unsure of the way forward for EERM technology

- 46% are unsure of the way forward for EERM technology

Use or plan to use cloud-based platforms for EERM

- 45% use or plan to use cloud-based platforms for EERM

Focus on RPA

- 36% focus on RPA

Use or plan to use cognitive analytics or visualization techniques

- 25% use or plan to use cognitive analytics or visualization techniques
Leveraging external assistance
A growing number of organizations use external support to improve and supplement their EERM programs. That includes assistance with risk intelligence, utility models, and managed services.

By last year’s survey, more federated EERM models had started to dominate, underpinned by a center of excellence (CoE) or shared service structure (SSC) for TPRM. This trend has continued this year.

- **57%** of respondents already use or intend to establish a CoE
- **54%** already use or intend to establish an SSC

![Diagram](image)

Nearly a quarter of organizations (24%) are at least partially outsourcing CoEs and SSCs. This is a significant shift from five years ago, when nearly all CoEs and SSCs were fully in-house.

1. **Although in-sourcing of processes may offer an attractive short-term option to regain control of critical processes,** use of external support for improving or delivering organizational EERM programs will be judicious in the months ahead.

2. **Going forward, technology-based managed services models and utilities will drastically reduce EERM capital costs (and to some extent operating costs) while improving the quality and rigor of risk-management efforts.**
Wider focus
Senior executives are extending their focus beyond risk to include a broader view of third-party management. This will enable synergies in the long term but creates coordination challenges during the transition.

1. We predict this evolution of a more strategic and broader view of third-party management will continue

2. We believe the trend for ultimate accountability to travel to the very top of the organization will improve coordination, which could otherwise prove to be a significant challenge
With the evolving digital landscape and increasing dependency on extended enterprise, the following upcoming trends will further strengthen and complement the point in time assessments that organizations undertake.

### Technology Enablement
- Implement technology solutions for data security
- Solutions such as Digital Rights Management and Vendor Identity Access Management Systems
- Leverage Analytics for intelligence gathering and make EERM program an effective one

### Risk sensing approach & Risk exchange utility
- BitSight Security Ratings can help evaluate vendor’s security performance by continuously analyzing, and monitoring companies’ cybersecurity, all from the outside.
- Third Party Risk Exchange Utility such as CyberGRX is an emerging trend. 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.

### Continuous Monitoring
- Focus on enhancing the maturity of their EERM program and look beyond point-in-time assessments.
- Ongoing monitoring of the KRIs. Monthly KRI dashboard.
- Enforce vendors to implement effective controls, enhancing their security posture.
EERM trends - What You should Expect Next? (2/2)

With the evolving digital landscape and increasing dependency on extended enterprise, the following upcoming trends will further strengthen and complement the point in time assessments that organizations undertake.

- **Integrated assessments**
  - Shift in the risk evaluation of Third Parties – Increased coverage of domains including 4th Parties, Financial solvency, Performance management etc.

- **Risk analysis & prioritization**
  - Risk profiling is critical, allocation of limited manpower, budgets and resources

- **Accountability moving to the top**
  - Top-level accountability will make it easier for people in charge of different risks, business unit leaders, functional heads, legal teams, internal audit, and so on, to work together.
Challenges resolved with Technology Enablement

The Risk landscape is constantly evolving with new risks and response strategies around every corner. These challenges and opportunities demand a value-focused approach to risk management and strategies around modernizing risk functions and practices.
Thank you