Internal Audit’s Role in Third Party Risk Management (TPRM)

Jon Pastore, Nick Fullmer
Third Party Risk Management (TPRM) Framework

What is Third Party Risk Management?
Third Party risk management is focused on understanding and managing risks associated with third parties with which the company does business and/or shares data.

Why is Third Party Risk Management Important?

Elements of Third Party Risk Management program

What is the role of Internal Audit in TPRM programs?

Common challenges with TPRM Audits

Successful Internal Audit TPRM activities

The PwC TPRM Framework

Risk Considerations

<table>
<thead>
<tr>
<th>Reputational</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational</td>
<td>Regulatory / Compliance</td>
</tr>
<tr>
<td>Financial</td>
<td>Physical Security</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>Subcontractor</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>Technology</td>
</tr>
<tr>
<td>Information Security</td>
<td>Concentration</td>
</tr>
<tr>
<td>Country</td>
<td></td>
</tr>
</tbody>
</table>
**Vendor Management (VM) vs. TPRM**

**What is Third Party Risk Management?**

Vendor management accounts for the enterprise-wide relationships and the potentially numerous products/services that the third party may provide, including the service level and risk aspects. TPRM risk activities are conducted in parallel to the vendor management relationship and service level activities.

### Vendor Management (VM) life cycle

<table>
<thead>
<tr>
<th>VM life cycle</th>
<th>Planning</th>
<th>Due Diligence</th>
<th>Contract Negotiation</th>
<th>Ongoing Monitoring</th>
<th>Relationship exit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5. Determine Third Party Base</td>
<td>- Existing</td>
<td>5. Price vs Value</td>
<td>5. Transition Planning and Execution</td>
<td></td>
</tr>
<tr>
<td><strong>For critical activities, involve appropriate levels within the organization</strong></td>
<td></td>
<td>- Proof of Concepts</td>
<td>10. For critical activities, involve appropriate levels within the organization</td>
<td>10. Finalize Exit Strategy</td>
<td></td>
</tr>
</tbody>
</table>

### Third Party Risk Management (TPRM) life cycle

<table>
<thead>
<tr>
<th>TPRM life cycle</th>
<th>Planning</th>
<th>Due Diligence</th>
<th>Contract Negotiation</th>
<th>Ongoing Monitoring</th>
<th>Relationship exit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Cost Benefit Analysis</td>
<td>- Competitive Bid</td>
<td>- MSA</td>
<td>2. Provide Notifications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Determine business requirements</td>
<td>- RFP/RFQ</td>
<td>- SoW</td>
<td>3. Risk Exposure assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6. Determine inherent risk</td>
<td>- Potential</td>
<td>4. Clauses to address open issues</td>
<td>6. Transfer of assets and Information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10. For critical activities, involve appropriate levels within the organization</td>
<td>- Proof of Concepts</td>
<td>8. Determine residual risk</td>
<td>10. Finalize Exit Strategy</td>
<td></td>
</tr>
</tbody>
</table>

**Elements of Third Party Risk Management program**

**What is the role of Internal Audit in TPRM programs?**

**Common challenges with TPRM audits**

**Successful Internal Audit TPRM activities**
Regulatory Considerations

Over the last 20+ years, multiple new regulations across industries have demanded increased focus on how organizations monitor their third parties.

What is Third Party Risk Management?

Why is Third Party Risk Management important?

Elements of Third Party Risk Management program

What is the role of Internal Audit in TPRM programs?

Common challenges with TPRM Audits

Successful Internal Audit TPRM activities

Regulatory changes in certain sectors may also have a down-stream impact on business partners.
Reputational Drivers for TPRM

Sample headlines involving Third Parties:

**CFPB Orders $59.5 Million Fine for Illegal Credit Card Practices**

The Consumer Financial Protection Bureau (CFPB) ordered a large credit card provider to refund an estimated $59.5 million to more than 335,000 consumers for illegal credit card practices after they discovered three subsidiaries, their vendors and telemarketers engaged in misleading and deceptive tactics to sell some of the company’s credit card add-on products.

**Hackers Used Third Party Log-on to Steal Data and E-mails**

Hackers used stolen credentials from a third party to gain access to a retailer’s network, where they exploited an unpatched vulnerability in the system to gain access to point-of-sale data. As a result, around 56 million payment cards accounts and 53 million email addresses were stolen.

**Attackers Broke in via HVAC Company**

Attackers first broke into a leading retailer’s network using network credentials stolen from a provider of refrigeration and HVAC systems. As a result, 70 million people were affected and the stolen customer information included names, mailing addresses, phone numbers as well as email addresses.

**Breach by Vendor Awakens New Insider Threat Concerns**

Employees of a third party service provider violated privacy guidelines by accessing, without authorization, consumer accounts as part of a scheme to obtain customer names and partial SSNs, which were used to request unlock codes for stolen mobile phones. As a result of the breach, service provider agreed to settle an FCC investigation and pay a $25 million fine.

**$1.55 million settlement underscores the importance of executing HIPAA business associate agreements**

An investigation indicated that the hospital failed to have in place an appropriate business associate agreement, as required under the HIPAA Privacy and Security Rules, so that its business associate could perform certain payment and healthcare operations activities on its behalf.

**Recent Ponemon Institute surveys reveal:**

- Approximately half the respondents (49%) confirm their organization experienced a data breach cause by one of their vendors.
- 73% of the respondents see the number of cybersecurity incidents involving vendors increasing. 65% of the respondents also say it is difficult to manage cybersecurity incidents involving vendors.

What is Third Party Risk Management?

Why is Third Party Risk Management important?

Elements of Third Party Risk Management program

What is the role of Internal Audit in TPRM programs?

Common challenges with TPRM audits

Successful Internal Audit TPRM activities
Third Party Risk Management (TPRM) Lifecycle

- **What is Third Party Risk Management?**
- **Why is Third Party Risk Management important?**
- **Elements of Third Party Risk Management program**
- **What is the role of Internal Audit in TPRM programs?**
- **Common challenges with TPRM Audits**
- **Successful Internal Audit TPRM activities**
A TPRM strategy is supported by three lines of defense – the first line lies within each individual Line of Business and is empowered by the second line who owns the provision of ongoing guidance, tool support, and facilitation of cross-business collaboration. The third line is responsible for evaluating the design and operating effectiveness of the Program.

### C. Third Line of Defense
- Independently test, verify and evaluate risk management controls against internal policies
- Report upon effectiveness of the program

### B. Second Line of Defense
- Design and assist in implementing company-wide risk framework and oversee enterprise risks
- Perform quality reviews and other targeted oversight practices to ensure that the line of business is compliant with internal policies/external regulations

### A. First Line of Defense
- BU managers and third party relationship owners are responsible for identifying, assessing and mitigating risk associated with their business
- Implement internal controls and practices that are consistent with company-wide policies & procedures
Upon identification of a potential product/service to outsource to a Third Party, organizations should ensure there is a plan to manage the relationship. This plan should start by identifying the inherent risk profile of the product/service to be outsourced.

Prior to contract execution, organizations should conduct a review of potential third parties in order to select a Third Party with the appropriate qualifications, and to understand the Third Party’s controls to mitigate the inherent risks posed by the relationship.

The contract should clearly define expectations and responsibilities of the Third Party. The inclusion of appropriate contract clauses help to ensure the contract’s enforceability, limits the organization’s liability, and mitigates disputes about performance.

Post contract execution and ongoing monitoring should include both risk and performance management. Issues should be identified, remediated, and escalated to appropriate decision authorities. Contingency plans should be maintained to ensure the activities can be transitioned in-house or to another Third Party.

Termination may be required when a contract expires, the terms of the contract have been satisfied, in response to contract default, or in response to changes to the organization’s or Third Party’s business strategy. The organization should execute against written contingency plans to mitigate risk during termination.
Planning – Third Party inventory and stratification

The inventory, risk rating and ongoing testing model enables a focus on efforts to establish the third party inventory, oversee services with higher levels of inherent risk. The model drives the ongoing due diligence process based on the inherent risk and the nature of the services provided.

What is Third Party Risk Management?

Why is Third Party Risk Management important?

Elements of Third Party Risk Management program

What is the role of Internal Audit in TPRM programs?

Common challenges with TPRM Audits

Successful Internal Audit TPRM activities
Establishing third party inventory

This framework will assist the Third Party Risk Management Program in honing in on the inventory list by analyzing multiple sources in rapid manner and identifying the third parties that need to be included as part of the program, and rated by inherent risk.

Begin with A/P spend and LOB files to identify “Vendors” and “Special Categories”. Remove those that don’t pose risk.

Identify unique third parties and validate services against existing invoices & data sources. Remove those that don’t pose risk.

Perform cleansing and enhancement of third party data

In-scope third party inventory for risk segmentation

Inherent risk assessment

Inherent Risk Rating

Starting with commodity categories, we use a process to focus on those products/services that do and do not pose inherent risk and thus to be included as part of the program.

We then clean and enhance the existing third party data to be put into the inventory repository.

Common Third Inventory Data Attributes

- Third Party Name
- Third Party Parent Name/Associated Third Parties
- Product/Service
- Third Party Type (Business Process Outsourcing, Partnership, Technology etc.)
- Spend
- Business Lines/Processes Supported by the Third Party
- Country/Region where Third Party is Based
- Contract Date (Engagement Date)
- Results of Third Party Risk Classification
- Results of Third Party Risk Assessments (e.g., Third Party Information Security Assessments)
Inherent risk assessment

The inherent risk assessment process allows for the sorting of third party services/products inherent risk scores and inherent risk ratings.

Risk stratification structure

1 – “High Risk” These third parties are handling high risk services, have a critical level of disruption, access to highly restricted types of data and are client facing.

2 – “Moderate Risk” These third parties are handling high or medium risk services, have high level of disruption, access to restricted data and may be client facing.

3 – “Low Risk” These third parties are handling medium risk services, have a moderate level of disruption, have access to restricted data and are not client facing.

4 – “Very Low Risk” These third parties are handling low risk services, have a low level of disruption, do not have access to restricted data and are not client facing.

Elements of Third Party Risk Management program

What is Third Party Risk Management?

Why is Third Party Risk Management important?

What is the role of Internal Audit in TPRM programs?

Common challenges with TPRM Audits

Successful Internal Audit TPRM activities

Inherent risk determination

Service Inherent Risk

Financial

Information Security

Legal & Regulatory Compliance

Business Continuity

Privacy

Reputational

Reputational
Third party stratification and assessment model

The inherent risk determination should be dictate what initial and ongoing due diligence activities are required based on input from applicable Subject Matter Specialists groups.

**Inherent risk determination**

<table>
<thead>
<tr>
<th>Pre-Sourcing</th>
<th>Example Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Legal</td>
</tr>
<tr>
<td></td>
<td>Third Party Risk Office</td>
</tr>
<tr>
<td></td>
<td>Subject Matter Specialists</td>
</tr>
<tr>
<td></td>
<td>Business Unit Sponsor</td>
</tr>
<tr>
<td></td>
<td>Compliance</td>
</tr>
<tr>
<td></td>
<td>Sourcing &amp; Other Key Stakeholders</td>
</tr>
</tbody>
</table>

**Initial due diligence activities performed during pre-contract utilizing and SMS input**

- **Legal** should advise on potential sourcing of critical activities and when negotiating any contract or service agreement.

- The **TPRM Office** will assist with the execution of pre-contract and ongoing due diligence assessments.

- Subject Matter Specialists (e.g., InfoSec, BC/DR, Compliance, etc.) will either have input or will perform the pre-contract due diligence assessment from the perspective of the specialized risk area.

- **Business unit sponsors** will be required to complete the inherent risk assessment and exit plan if required.

- **Compliance** will assist in determining applicable laws and regulations.

- **Sourcing** will advise the business in areas of strategic sourcing initiatives, and maintain process alignment with sourcing strategy.
Third party risks in relation to assessments

The following correlates significant third party risks to the assessments utilized by organizations to evaluate the effectiveness of third party controls in place to mitigate risks.

**What is Third Party Risk Management?**

**Why is Third Party Risk Management important?**

**Elements of Third Party Risk Management program**

**What is the role of Internal Audit in TPRM programs?**

**Common challenges with TPRM Audits**

**Successful Internal Audit TPRM activities**

---

**Compliance:**
Assesses the third party’s ability/control framework in place to comply with laws/regulations.

**Information Security & Privacy:**
Assesses third party controls over the availability, confidentiality, and integrity of third party data.

**Physical Security:**
Assesses facility access and security measures implemented by the third party.

**Country Risk:**
Assesses political, geographic, regulatory, legal, and economic risks of sourcing to a country or region.

**Reputational:**
Assesses the impact to the organizations reputation based on services provided by a third party.

**Operational Competency:**
Assesses the ability of the third party to deliver the contracted products/services.

**Subcontractor:**
Assesses the risk management processes surrounding the use of subcontractors by third parties.

**Technology:**
Assesses the adequacy and appropriateness of the third parties systems and applications to provide the product/service.

**Financial:**
Assesses financial stability for the third party to continue provide the product/service.

**Business Continuity & Resiliency:**
Assesses the third parties ability to perform in the event of a process failure or catastrophic event.
The following are examples of Third Party due diligence assessments performed on potential and existing third parties to understand the existing control environment and capabilities.

**Risk assessment types**

- **Information Security & Privacy**
  - Security policies
  - Change controls
  - Encryption
  - Logical access Control
  - Monitoring, communication and connectivity
  - Incident management
  - Application management
  - System development
  - Customer contact

- **Technology**
  - Technology Architecture
  - Assets utilized
  - Technology Roadmap
  - Technological capabilities

- **Physical Security**
  - Fire Suppression
  - Server Security & Conditions
  - Data Centers
  - Backup Power Sources
  - Asset management
  - Key Card & Facility Access

- **Subcontractor**
  - Third Party Relationship Management
  - Sub-Service Third Party Relationships
  - Logical access Control
  - Monitoring, communication and connectivity

- **Country**
  - Political
  - Geographic
  - Regulatory
  - Legal
  - Economic
  - Travel Safety

- **Reputational**
  - Litigation or ethical flags
  - Media coverage
  - OFAC or other factors
  - Criminal and/or civil complaints

- **Financial**
  - Going concern
  - Liquidity
  - Leverage
  - Profitability
  - Transaction Processing

- **Compliance**
  - Regulatory requirements
  - HIPAA
  - CFPB
  - GLBA
  - Customer complaints handling, PCI

- **Business Continuity & Resiliency**
  - Recovery
  - Data Backup Management
  - Offsite storage
  - Media and vital records
  - Data integrity

---

*Business Continuity Management includes Business Contingency ("BC") planning and Disaster Recovery ("DR")*
Due diligence – Leveraging SOC 2 + reporting

A SOC 2 + can provide an efficient and effective solution to facilitate burdensome third party assessments. It can enable you to reduce costs associated with accommodating multiple TPRM questionnaires and on-site TPRM assessment procedures.

Challenges with prior solutions

- Questionnaires used by most organizations are large and open to interpretation
- Assessments are performed at the point of time
- No clear linkage between questions and risks being addressed

SOC 2 + framework

- SOC2 report framework based on the AICPA guiding principles with insight for third party industry best practices
- Criteria agreed upon by the audit team and the organization (third party) that address customer concerns, outside of the scope of standard SSAE16/SOC1 and SOC2 control testing environments
- Conducted by independent firm

Benefits to the organization

- Reduces time and money spent on resources
- Offers more time to proactively address risks
- Improves management of costs
- Decreases the number of on-site audits
- One to MANY reporting and remediation relationships as compared to the current customer Third Party Risk Management response process

Benefits to clients

- Reduces time and money spent on resources and travel
- Helps restore confidence
- Provides positive and independent analysis across a period of time, not just a point-in-time
- Reduces time for the assessment lifecycle
Due diligence and contracting

In addition to generating a risk rating/segment based on the inherent risk of the relationship to your organization, the results of your pre-contract due diligence should drive contractual protections.

**Example Contract Clauses**
1. Nature and scope of service
2. Performance standards
3. Subcontracting & 4th Parties
4. Diversity
5. Indemnification
6. Default and termination
7. Confidentiality & Security
8. Regulatory requirements
9. Ownership, license and access
10. Business continuity and contingency planning
11. Controls verification
12. Notification & escalation procedures
13. Limits in Liability
14. Insurance
15. Right to Audit
16. Records management
17. Pricing
18. Cost and compensation
19. Payment terms
20. Dispute Resolution
21. Management Information Systems reporting responsibilities
22. Customer complaint handling
23. Amendments

*Business Continuity Management includes Business Contingency (“BC”) planning and Disaster Recovery (“DR”)*
Ongoing Monitoring

Inherent risks should drive the nature, timing and extent of activities used to monitor, oversee, and re-assess Third Party relationships.

Depth and Frequency of Ongoing Monitoring

- **Very Low (40-50%)**
- **Low (20-30%)**
- **Moderate (10-15%)**
- **High (3-5%)**

**Risk Scorecards / “Satisfaction Surveys”**

**SLA Tracking**

---

**What is Third Party Risk Management?**

**Why is Third Party Risk Management important?**

**Elements of Third Party Risk Management program**

**What is the role of Internal Audit in TPRM programs?**

**Common challenges with TPRM Audits**

**Successful Internal Audit TPRM activities**

---

PwC IIA Milwaukee Chapter Roundtable March 2018
Termination

Each third party termination will be unique; however, there are common decisions, considerations, and results that should be addressed with key stakeholders and executed with a defined plan and checklist.

Termination decision
- Service Failure/Significant Customer Complaints
- Data Breach/Security Incident
- Regulatory/Legislative
- End of Contract
- Business Decision
- Product/Service Discontinued

Termination considerations
- Product/Service Brought In-House
- Product/Service Transitioned to Alternate Third Party
- Customer Impact
- Operational Impact
- Patient Safety
- Contingency Procedures
- Oral & Implied Contracts
- Internal Employee Impact

Termination result
- Interim Processes
  - NDA
  - Transfer Process Knowledge
  - Migrate or Destroy
- Information
  - Return or destruction
  - Ongoing safeguards
  - Ownership and control
- Costs
  - Monetary
  - Non-monetary
- Migrate/Sell Assets
  - Software/Intellectual Property
  - Hardware
  - Facilities
- Notification to Customers and Employees
Full Room Discussion 1

Activity: Discuss your organization’s approach to internal audits related to TPRM or third parties, including:

A. Scope or focus of audits
B. Frequency of these types of audits
The role of internal audit is to perform two distinct services: (i) independently evaluate the effectiveness of the program and (ii) ensure the program is doing the “right” things.

Internal Audit
- **IA must be independent** and should examine whether the deployed TPRM Program controls are designed properly and are operating as designed, as related to activities occurring at the third party locations.
- **IA should consider recent regulatory guidance and industry recommended practices** when reviewing the TPRM Program to ensure the organization is focusing on the “right” things.
- **IA’s focus is typically on the more significant relationships** from an inherent and residual risk perspective based on the second line of defense’s risk assessments.
- IA being the third line of defense, **should not be influenced** by what TPRM or Subject Matter Specialists may have completed.
Questions to Consider

What is Third Party Risk Management?

Why is Third Party Risk Management important?

Elements of Third Party Risk Management program

What is the role of Internal Audit in TPRM programs?

Common challenges with TPRM Audits

Successful Internal Audit TPRM activities

Governance
- Who is accountable for oversight and the overall management of your Third Party Risk Management (TPRM) Program?
- Are roles and responsibilities across the enterprise clearly delineated and adhered to?

Planning
- Do you have an inventory of existing Third Parties?
  - Are they categorized by product/service?
  - Are each risk ranked?
- Do you have current contracts related to the product/service being provided?
- Do Third Parties go beyond traditional vendors and suppliers (e.g., joint ventures, affiliates)?
- Are there standardized risk profiling methodologies with defined assessment frequencies and types in place?

Due Diligence and Third Party Selection
- Are due diligence assessments performed prior to contracting?
  - What risk areas are considered (e.g., information security, compliance, business continuity, reputation, etc.)?
- Do you know which of your third parties have access to data?
- Do you know which subcontractors are used by your third parties, and what work they are performing for you?

Contract Negotiation
- Do contract clauses include the “right to audit” the Third Parties processes’ over the service provided?
- Are contracts for similar services consistent and contain Service Level Agreements?

Ongoing Monitoring
- Do monitoring processes include both risk AND performance concerns?

Termination
- Do you have exit strategies in place for significant/high risk Third Party relationships?
Full Room Discussion 2

**Activity:** Discuss TPRM program audits, including:

A. Challenges experienced in performing these types of audits

B. Success stories
Common Challenges with TPRM Audits

Example pitfalls when performing independent reviews include:

• Auditing perceived high risk vendors without auditing the program or process
• Focusing on Third Party spend instead of risk
• Not applying same level of scrutiny as regulators (e.g. OCC TPRM Examination Procedures).
  For example:
  o Board approved policy
  o Identification of process exceptions (e.g., Due diligence not completed prior to Contracting)
  o Risks beyond Information Security and Business Continuity
  o Ongoing monitoring activities above and beyond periodic re-assessments
  o Trust but verify
• Not thinking broadly enough, (i.e., is the scope of the TPRM program complete?)
• Focusing on completion of activities by the 1st and 2nd line instead of the quality of the activities and the skills and capabilities of the individuals managing the risk
Successful Internal Audit TPRM Activities

Internal Audits of TPRM programs throughout the various stages of maturity and operation can drive significant value to the organization. Examples of successful, enterprise driven results include:

- Identification of breakdown in enterprise wide TPRM activities throughout the TPRM lifecycle. The audit drove an enterprise initiative to collaboratively develop an enterprise wide program with formalized ownership and consistent processes.

- Uncovered inconsistent execution of requirements across business units. Resulted in enterprise procedures and templates being developed to enable consistency across a federated model.

- Raised gaps in regulatory compliance prior to formal examinations. Identified issues created urgency and drove management focus to enhance design and operationalization of TPRM activities within an accelerated timeframe.

- Identified areas of success in specific risk dimensions, but absence of oversight in other key areas. This resulted in a revision and expansion of TPRM program focus to include other dimensions that were not initially addressed.

- Determined gaps in third party inventory as well as opportunities for enhancement in the payment control processes. The efforts resulted in refinement to onboarding and payment processes as well as better connection between risk, payment and contracting systems.
Questions?
Wrap Up and Closing Remarks