Third Party Oversight...

Bless me Father for I have sinned

We make sales calls after 9:00 PM everyday

I like what you’ve done with our third party risk program

We cannot just hope our third parties will do the right thing
Key topics for this session

- Third Party Risk Management: An End to End Review
- Case Study
- Lessons Learned

Why is Third Party Risk Becoming so Important

In the past third party risk management performed mostly by very large organizations and was primarily focused on supply chain. Now third party risk has made become an important topic with senior leaders and the board.

1. **Availability of low-cost third party options** has increased significantly and organizations now have access to a multiple highly skilled, economic service providers that compete aggressively in the global market.

2. **Outsourcing of critical business functions and products/services** to focus on core competencies and services. This creates a greater level of dependence on third parties as the ability to bring certain products and services.

3. **Regulatory and auditor scrutiny has increased** due to technology advances that can produce a variety of products and services across the globe. This expansive reach of third parties exposes organizations to laws outside of the US.

4. **Highly visible data breaches and events** have changed the regulatory landscape in a significant way. For example, the Bank failures in 2008 drew significant criticism against both the institutions and regulators for a lack of oversight. After this event there was significant pressure to improve identification and monitoring of risks.
Understand your Third Party Environment

Starts with simple yet often times difficult questions to answer.

1. Who are your third parties and their subcontractors?
2. What business are we doing with them and why?
3. Which relationships expose your company to risk and to what risks?
4. What is the criticality of these risks to your organization and to individual business units?
5. How are we identifying, reporting and remediating these risks?

Questions your Governance team needs to be asking

Understand Regulatory Requirements

1. Continued focus on managing Compliance and Privacy risks related to your third parties
2. Information Sharing between public and private sectors getting a hard look
3. Compliance of consumer information laws and regulations is back in the spotlight
4. Increasing the depth and breadth of due diligence requirements

Longer standing requirements...
- HIPAA
- FDCPA
- OFAC
- GLBA

Recent requirements...
- OCC Cybersecurity Statement – 2020
- CCPA – 2020
- NY DFS Regulation 500 – 2019
- FDA CGMP Data Integrity Standards – 2018
- EU GDPR – 2018

What impact has it had…and what’s next?
- Cost of compliance has become an issue
- Compliance requirements keep increasing
- Company's are looking for ways to be more efficient and look ahead to cover critical risks
Third Party Operating Framework

**Identify**
- Third parties
- Services
- Risks
- Rank by criticality (impact, likelihood)

**Mitigate**
- Pre-contract due diligence
- On-site reviews (critical third parties)
- Desktop reviews (lower rated risks)
- Daily new feeds (reputational risks)
- Issue identification & remediation

**Monitor**
- Post contract due diligence based on criticality
- Daily news feeds (reputational risks)
- On-site reviews (critical/high third parties)
- Desktop reviews (lower rated risks)
- Issue identification
- Remediation

---

Identify your Third Party Population

Regulators and auditors have an expansive definition of third party – “A third party is any relationship between your company and another entity through a contract or otherwise”. Reality Check – any relationship you have that may cause a reputational or regulatory risk to your firm.

Goes Beyond Your Typical Suppliers

- Suppliers
- IT Providers
- Payment Processing Partners
- Strategic Partnerships
- Law Firms
- Joint Ventures
- Distribution Agents
- Affiliates
- Data Exchanges

Understand the criticality & risk(s) so you can most appropriately perform due diligence
Mitigate Higher Risk Engagements

What third party risk factors qualify for more in-depth assessments?

### Third Parties
- Service will interact directly with customers and have the ability to influence existing or perspective customers.
- Service will have the ability to influence, without two-way interaction, to customers, e.g., marketing promises.
- Store, process, or transmit personal data (internal, customer, etc.) on their own IT systems and network.
- High operational dependency to maintain sales, customer satisfaction, etc.

<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>Due Diligence Requirements</th>
<th>Recurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>On-site Assessment</td>
<td>Annually</td>
</tr>
<tr>
<td>Moderate</td>
<td>Remote Assessment</td>
<td>Bi-annually</td>
</tr>
<tr>
<td>Low</td>
<td>Self Assessment</td>
<td>Contract Renewal</td>
</tr>
</tbody>
</table>

### Data Sensitivity
Shared with/collected by/accessible to the third party:
- Customer information and prospective customer information.
- Employee, employee family, applicant, and contractor personal identifiable information.
- Organization’s intellectual property, proprietary information, and financial data, technical data/IP addresses.

#### Residual Risk Model

<table>
<thead>
<tr>
<th>Inherent Risk</th>
<th>Last Review Rating</th>
<th>Residual Risk</th>
<th>Review Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Satisfactory</td>
<td>High</td>
<td>Annually</td>
</tr>
<tr>
<td>Medium</td>
<td>Satisfactory</td>
<td>Moderate</td>
<td>Bi-annually</td>
</tr>
<tr>
<td>Low</td>
<td>Satisfactory</td>
<td>Low</td>
<td>Contract Renewal</td>
</tr>
</tbody>
</table>

Third Parties
- Customer information and prospective customer information.
- Employee, employee family, applicant, and contractor personal identifiable information.
- Organization’s intellectual property, proprietary information, and financial data, technical data/IP addresses.

#### Illustrative Examples

**Inherent Risk Model**

**Residual Risk Model**

**Monitory with the Right Type of Governance**

- Consists of executive leaders from the business, risk, compliance, operations, etc.
- Responsible for approving the strategic direction of the company's risk programs.
- Responsible for reviewing critical risks and escalated issues and making business decisions based on those risks.
- Provides top-down alignment of risk activities for dashboards and metrics.

- Consists of mid-level leaders from the business, risk functions, legal, operational risk and third party risk management.
- Responsible for defining the TRPM program requirements and strategies.
- Reviews higher risk supplier contracts, risk mitigation strategies and escalated issues; provides decisions to TRPM operations and escalates to enterprise risk committee.
- Defines execution strategies to present to the third party risk operating group.
- Responsible for executing the TRPM operations and facilitating risk assessments and ongoing monitoring of third parties.
- Provides risk and reporting expertise along with the operational skillsets to execute risk activities effectively and efficiently.
Case Study

Client Background

Fortune 100 diversified financial services group of companies including an inter-insurance exchange and subsidiaries offering banking, investing, and insurance. The organization currently has over 20 million members.

- Lack of formal third party governance for compliance risk.
- Missing segmentation of compliance for higher risk third parties.
- Internal resources were not staffed to handle the assessment workload.
- Needed to develop an internal plan and approach to assess critical and high risk third parties.

| Large financial organization | ~34,000 Employees |
| ~$31 billion Revenue in USD  | ~20.8 million Members |
**Timeline of Third Party Compliance Reviews**

Grant Thornton has worked with the client to define, pilot, and execute third party compliance assessments for their critical and high risk third parties for over a year, based on regulatory and Internal Audit findings.

- **January 2019**: Pilot TP Onsite Compliance Assessments
  - Assisted with defining the onsite assessment process and performed onsite assessments of 4 higher risk third parties

- **April – Dec 2019**: TP Compliance Remote Reviews
  - Assisted with an influx of remote assessments for moderate risk third parties to supplement existing team

- **Oct 2019 – Jan 2020**: TP Onsite Compliance Assessments
  - Performed onsite assessments of 23 higher risk third parties in-scope for 2019

- **Jan 2020 Start**: 2020 TP Onsite Compliance Assessments
  - Execute onsite compliance assessments for 2020 in-scope third parties

---

**Scoping Approach for Onsite Assessments**

The scoping process included a review of contractual obligations, along with any identified regulatory requirements based on the contract and service type. In partnership with the client's legal department, we then validated the requirements with business and compliance stakeholders to determine internal and external responsibility, and which higher risk requirements to include in the draft assessment plans.
**Compliance Onsite Assessment Process**

The engagement workflow below was customized for the clients specific needs, however it is similar to standard workflows used across many client and industries. The onsite review process generally lasts between 2-6 weeks, where longer durations are usually due to third party delays and scheduling.

<table>
<thead>
<tr>
<th>Scope*</th>
<th>Planning</th>
<th>Onsite Preparation and Execution</th>
<th>Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Risk Control Matrix</td>
<td>Formulate test steps</td>
<td>Conduct kick-off call</td>
<td>Send request list to third party</td>
</tr>
<tr>
<td>Schedule onsite</td>
<td>Onsite assessment execution</td>
<td>Determine gaps in control testing</td>
<td>Draft issues</td>
</tr>
<tr>
<td>1 – 3 weeks</td>
<td>1 – 3 weeks</td>
<td></td>
<td>Complete assessment report</td>
</tr>
</tbody>
</table>

*Depending on the scope of the TPRM program and associated risk assessments, there might be standard assessment questionnaires to use. Within the security domain for example, NIST CSF and ISO27001 are common control standards.

---

**Value Driven Results**

The compliance onsite program has been well received across the organization and their third parties. It has also identified valuable process improvement opportunities with current providers.

- **Value Delivered from the Assessment Process**
  - **Expertise**
    - Compliance SMEs across all business lines
    - Regulatory insight to assist compliance with requirements
    - Industry knowledge on how others are complying
  - **Speed**
    - Ability to assess due diligence quickly prior to onsite visit
    - Dedicated PMO improves communications with business and third parties
  - **Scale**
    - Ability to quickly assign staff to conduct onsite assessments
    - Multiple assessments occurring simultaneously
    - Ability to scale up or down based on volume
  - **Quality**
    - Multiple layers of quality assurance checks
    - Accuracy of findings and documentation for both control effectiveness testing and control design evaluation

- **Lessons learned that will improve future efficiency and effectiveness:**
  - Scoping of compliance requirements for each service type requires alignment with 1st line, 2nd line, and the business
  - There’s a need to manually understand the service being performed by the third party, as contracts and SLA’s may not always be accurate
  - Data analytics are beneficial to identify compliance trends across business units, products, and outsourcing service types (e.g., subcontractors & licensing requirements)
Parting Thoughts

1. Third Party Population
   Define your full population of third parties and services being provided and consistently segment them based on risk.

2. Governance
   Governance, risk escalation, and reporting are critical components. Understand the business objectives.

3. Risk-Based Approach
   Employ a risk-based segmentation of your third-party supplier base and rank your third parties and services by criticality.

4. 4th, 5th, Nth Parties
   Understand what third parties require subcontractors and the criticality of those subcontractors to your operations or service delivery.

5. Automation
   Implement third party risk technology and integrate that technology to your supply chain and reporting engines. Drive consistency and efficiency into your process.

Questions?

Adam Schrock
Managing Director
adam.schrock@us.gt.com

Mike Pankey
Senior Manager
mike.pankey@us.gt.com
Grant Thornton's Third Party Risk Experience

**Experience**
- National TPRM Practice
- 200 resources dedicated to third party risk management assessments and attestations
- Past Regulator Expertise

**National Practice:**
- Certified / trained practitioners
- Offshore support team
- Strategic alliances with leading third party risk technology vendors (OneTrust, Coupa Risk Assess, SAI Global, Archer, IHS-Markit, Process Unity, ServiceNow)

**Program Enablers**

**Intellectual Property:**
- TPRM diagnostic that harmonizes leading risk requirements and quickly assesses maturity of program
- Risk taxonomy and inherent/residual risk models
- Audience specific risk key performance metrics and dashboards
- TPRM Internal Audit RACM based on regulatory guidelines and leading practices
- Program Performance Metrics
- Pre-built risk questionnaires and controls for each risk domain

**Thought Leadership**
- TPRM conference presentations
- TPRM webinars & industry roundtables
- Whitepapers

---

Find out more by visiting: [http://gt-us.co/2u3S2wW](http://gt-us.co/2u3S2wW)