Optimizing Third-Party Risk
(Comply with Confidence, Execute with Efficiency)

September 24, 2015

Dennis J Frio
FS National Director
Third Party Risk Practice Leader

John J Swanick
National Insurance Advisory Practice Leader
BAS Partner
Agenda

• Expense Management
  – Core Challenges
  – Framework and Key Components
  – Uses and Potential Roadblocks

• 3rd Party Risk Management
  – Understanding the Risks
  – Thoughts from Regulators
  – 3rd Party Risk Management Defined
  – Changing Landscape

• Internal Audit – Providing an Important Line of Defense
  – Asking the Right Questions/Diagnostic, Maturity Assessment
  – Independent Reviews

• Summary
Can your business partners answer these questions?

1. Who are your third parties and their subcontractors?

2. What business are you doing with them – and why?

3. Which relationships expose us to risk – and to which risk

Know Your Third Parties
Spend Management Framework

Department Goals
- Identify and achieve savings
- Budget & forecast accuracy
- Compliance to contract price and performance standards

Department Objectives:
- Cost & Quality
- Accountability
- Control/Efficiency
- Compliance/Cash Mgmt

3rd Party Risk Management
Work collaboratively with the Source to Pay departments to achieve desired objectives but also minimize the risk third parties may cause to the company's customers, their operations, their reputation and, ultimately, their financial viability.
As companies continue to outsource critical business functions, they are relinquishing more of their control environment to third parties. Without proper risk management oversight, these third parties may cause harm to a company’s customers, their operations, and their reputation.

### Use of 3rd Parties
- Business Process Outsource Providers
- Claims Processing
- SAAS Technology providers
- Data Centers
- Customer Support Providers
- Legal Representatives
- Clearing/Settlement Firms
- Document storage providers
- Printing and Mailing Services
- Subcontractors used by 3rd parties

### Roadblocks
- Lack the proper visibility on the full complement of third party services
- Fragmented responsibility over 3rd parties – lack of company wide governance
- Poor data - Differing processes; multiple vendor masters with duplicate entries
- Lack of central contract repository – triggers for contract end dates
- Limited technology around performance management
## Third Party Risk Summary

<table>
<thead>
<tr>
<th>Third Party Risks</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security / Data Privacy</td>
<td>Third party has insufficient experience &amp; controls to protect the company’s and customer’s information from unauthorized access, disclosure, modification, or destruction.</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>Third party cannot continuously maintain its services due to business disruption (e.g. ineffective redundancy procedures).</td>
</tr>
<tr>
<td>Financial Viability</td>
<td>Third party is not financially secure to continue to provide you services at acceptable levels.</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Third party lacks the proper security to prevent unauthorized access to its facilities, equipment and resources to protect from damage or harm.</td>
</tr>
<tr>
<td>Contract Compliance</td>
<td>Third party products, services, or systems are not consistent with your policies and procedures, agreed service levels, applicable laws, regulations, and ethical standards.</td>
</tr>
<tr>
<td>Legal/Regulatory</td>
<td>Third party does not possess the necessary licenses to operate &amp; the expertise to enable the company to remain compliant with domestic and international laws and regulations.</td>
</tr>
<tr>
<td>4th Party (Subcontractor Risk)</td>
<td>A fourth party contracted by the third party to service the client poses a additional risk for meeting its contractual requirements and other outlined risks mentioned above.</td>
</tr>
</tbody>
</table>
Quality of risk management over third-party relationships may not be keeping pace with the level of risk and complexity these relationships cause

- working with third parties that engage directly with customers
- outsourcing entire company functions to third parties, such as tax, legal, audit, or information technology operations
- outsourcing lines of business or products
- relying on a single third party to perform multiple activities, often to such an extent that the third party becomes an integral component of the company’s operations
- contracting with third parties that subcontract activities to other foreign and domestic providers
Regulators and even your key stockholders expect companies to have risk management processes that are appropriate for the level of risk and complexity their third-party relationships may cause.

Source: OCC 2013-29 Bulletin
# Third Party Risk Management

## Driving a Consistent Process

<table>
<thead>
<tr>
<th><strong>Planning/Risk Identification</strong></th>
<th><strong>Due Diligence/Third Party Selection</strong></th>
<th><strong>Contract negotiation</strong></th>
<th><strong>On-going Monitoring</strong></th>
<th><strong>Termination Procedures</strong></th>
<th><strong>Oversight &amp; Accountability</strong></th>
<th><strong>Documentation &amp; reporting</strong></th>
<th><strong>Independent Reviews</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop a plan that outlines the bank's strategy with regards to its third parties. Identify the inherent risks of the services and detail how the financial institution will select, assess and oversee their third parties.</td>
<td>Perform proper due diligence to identify potential risks before signing the contract. Understand the controls required and the risks the third party may pose to your organization.</td>
<td>Negotiate written contracts that clearly outline the expectations and responsibilities of third parties ensuring contracts enforceability, limits of liability and performance oversight.</td>
<td>Conduct on-going monitoring of the third party relationships focusing more attention on those parties who may pose the higher risk. Incorporate on-site reviews, audits as necessary.</td>
<td>Develop plan to transition the activities to another third party, bring activities in house or discontinue activities once contract is terminated.</td>
<td>Assign clear roles and responsibilities for overseeing and managing third party relationships. Ensure services deemed critical to your organization are visible at the highest level.</td>
<td>Maintain proper documentation and reporting to facilitate oversight, accountability, monitoring and risk management.</td>
<td>Conduct independent reviews of the risk management process to enable management to assess that the financial institution aligns with its strategy and effectively manages risks from third party relationships.</td>
</tr>
</tbody>
</table>

*Source: OCC 2013-29 Bulletin*
Planning/Risk Identification

• List of all third party vendors and services they provide (start with vendor master)
• Catalog vendor risks third party relationships may cause
• Segment your 3rd parties based on risk criticality

• **Critical activities** can be defined as those that...
  o have significant customer impacts
  o cause significant risks to operations if the third party fails to meet expectations – e.g. data privacy, business continuity,
  o requires significant investments in resources to implement the third party relationship and manage the risk (outsource a business function)
  o could have a major impact on the company's operations if an alternative third party is needed or of the outsourced activity has to be brought in house

With finite resources and budget, ensure time is spent on third parties that carry the highest inherent risk to your organization.
Third Party Risk Management
Consistent Vetting Process

TPRM requires a consistent approach to drive effort towards the most risky third parties. The process starts with an understanding of the complete listing of services consumed by your company with a mapping to what 3rd parties provide those services.

1. Will the 3rd party support a “critical” business process/service?
2. Will the 3rd party have direct contact with our customers?
3. Will the 3rd party have access to our internal network?
4. Will the 3rd party process, store, transmit or have access to customer and/or employee data?
5. Will the 3rd party use any subcontractors to deliver the requested services?
6. Will any service be provided by non-US locations?
7. Is the 3rd party headquartered outside the United States?
8. Will the third party impact our ability to comply with local government regulations?
9. Is the spend (one time or annual) greater than $100K?
10. Has the 3rd party provided a similar service with us before?

Illustrative

<table>
<thead>
<tr>
<th>Inherent risk score</th>
<th>Yes Response Triggers additional due diligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Residual Risk Score</td>
<td></td>
</tr>
</tbody>
</table>

Vendor Tiering

- 20,000 third parties [Low risk]
- 18,000 Low risk
- 1,700 Medium risk
- 300 High risk

Risk Management Programs

- Financial Viability
- Info Security/Data Privacy
- Legal/Regulatory
- Business Continuity
- Contract Compliance
- Physical/Personnel Security
- Management Programs
- 4th Party Risk (Subcontractors)
The degree of due diligence should be commensurate with the level of risk and complexity of the third-party relationship. Companies need to focus their efforts on the areas that present the greatest risks. On-site visits may be useful to understand fully the third party’s operations and capability to serve.

**Due diligence assessment criteria:**
- Audited Financial Statements
- Business reputation, complaints, and litigation
- Qualifications, backgrounds, and reputation of company’s officials
- Risk management procedures
- Compliance capabilities
- Internal audit coverage
- Technology and MIS sufficiency, business contingency plans
- Information Security
- Physical Security
- Reliance on sub-contractors
- Insurance coverage
Contract Negotiations

Senior Management should ensure that the expectations and obligations of each critical third party are clearly defined, understood, and enforceable.

**Note:** There tends to be time pressure to sign vendors so performing third party due diligence and contracting cannot be rushed at the expense of a good deal. Have contract templates already designed with key terms addressing identified risks.

**Common topics that should be included in contracts are:**

- Scope of the arrangement
- Performance measures or benchmarks
- Responsibilities - providing/receiving info
- Regulatory compliance requirements
- Costs and compensation
- Insurance
- Limits on liability
- **Business resumption/contingency**
- Default and termination
- OCC Supervision, if applicable
- **Sub-contracting**
- **Foreign Based third parties**
- Handling of Customer complaints
- Confidentiality and security
- Indemnification
- **Right-to-audit**
- "Balanced Scorecard"
A service-level agreement (SLA) is a part of a contract where a service is formally defined. Particular aspects of the service - scope, quality, responsibilities - are agreed between the service provider and the service user.

Common Service Level Agreements include:

- **Average Speed of Answer (ASA)** – Call Center – How long it takes to answer calls.
- **Claims Accuracy** – Claims Department – Accuracy of claims paid via the vendor
- **Turn Around Time (TAT)** – Claims Department – Length of time it takes to process a claim.
- **System Availability** – IT Systems – Vendor system availability.

Typically, SLA's can be reported monthly or quarterly.
Penalties for SLA are determined during contract negotiations. Contracts should detail what compensation you will receive if the vendor fails to meet its contractual obligations. The goal should not be to penalize, but ultimately to prevent problems from occurring in the first place and increase the probability of repeatable successes in the future.

Your compensation typically takes the form of an account credit, reducing the cost of vendor support for the following month. For example, you might receive a 5% credit for every hour the supplier fails to meet a target.

A good service level agreement should also provide a termination clause, if the supplier repeatedly fails to meet the SLA.
On-going Monitoring

After entering into a contract with a third party, company management should dedicate sufficient staff with the necessary expertise, authority, and accountability to oversee and monitor the third party with respect to its activities and performance.

**Performance monitoring may include:**

- Financial reviews for viability
- Ability to recover from service disruptions (resiliency)
- Ability to maintain confidentiality & integrity of a company's information (Personal Identifiable Information or PII)
- Physical security procedures
- Insurance coverage
- Agreements with other entities that may pose a conflict of interest or introduce reputation, operational, or other risks to the company
- Ability to appropriately remediate customer complaints
- Reliance on & performance of subcontractors
- Changes in key personnel; ability to retain essential knowledge to perform
- Changes to risk management procedures
Termination

Management should ensure that third party relationships terminate in an efficient manner, whether the activities are transitioned to another third party or brought in-house, or discontinued. In the event of contract default or termination, the company should have a plan in place that brings the service in-house if there are no alternate third parties.

This plan should cover:

• capabilities, resources, and the time frame required to transition the activity while still managing legal, regulatory, customer, and other impacts that might arise.

• risks associated with data retention and destruction, information system connections and access control issues, or other control concerns that require additional risk management and monitoring during and after the end of the third-party relationship.

• handling of joint intellectual property developed during the course of the arrangement.

• reputation risks to the company if the termination happens as a result of the third party’s inability to meet expectations.
The Changing Landscape

Current Practice

- Administrative burden on third parties contacted separately for the same risk data
- No standards to risk questions sent by multiple clients leading to inconsistent third party responses
- Costly annual process; redundant responses to multiple clients
- Inability to easily leverage responses to multiple clients for similar data

KY3P Utility™

- On stop for third party risk information including financial data, standard risk questionnaire responses, quality alert monitoring
- Consistent, repeatable process that drives more accuracy in third party responses
- Minimizes third party cost and effort to respond to multiple data requests from clients
- Promotes a consistent and repeatable risk management process
- Demonstrate - industry engagement and thought leadership to the regulators

3rd Parties | Clients
--- | ---
One-to-One | 3rd Parties
Many to One to Many | Clients

© Grant Thornton LLP. All rights reserved. 18
The company’s board of directors (or a board committee) and senior management should oversee the company’s overall risk management processes. There should be distinct roles and responsibilities set and escalation procedures communicated.

**Illustrative Structure**

- **Board of Directors**
  - Approve the company’s risk-based policies
  - Approve contracts that involve critical activities
  - Review and take action on significant deficiencies involving critical activities

- **Enterprise Risk Committee**

- **1st Lines of Business**
  - Owns the risk
  - Self assessments
  - Risk Remediation

- **2nd 3rd Party Risk Management**
  - Policies for 3rd party risk
  - Sets structure for risk program and escalation activities
  - Oversee risk assessments and remediation activity

- **3rd Internal Audit**
  - Perform periodic reviews
  - Highlight and discuss material risks and any deficiencies
  - Recommend improvement opportunities

**Note:** Prepares company for Regulatory Reviews
Proper documentation and reporting facilitates the accountability, monitoring, and risk management associated with third parties and typically includes:

- a current inventory of all third-party relationships, which should clearly identify those relationships that involve critical activities
- approved plans for the use of third-party relationships.
- due diligence results, findings, and recommendations.
- analysis of costs associated with each activity or third-party relationship, including any indirect costs assumed by the company.
- executed contracts.
- regular risk management and performance reports required and received from the third party (e.g., audit reports, security reviews, compliance with service-level agreements).
- regular reports to the board and senior management on the results of internal control testing and ongoing monitoring of third parties involved in critical activities.
- regular reports to the board and senior management on the results of independent reviews of the company’s overall risk management process.
Getting Involved – Internal Audit

- Do you understand **what services your 3rd parties provide** and which relationships expose our firm to the greatest risks?
- Do you employ a **risk-based segmentation of our third-party supplier base**?
- Do you understand which relationships **have access to or hold confidential company or client information**?
- Do you have a **disciplined governance and risk escalation process**?
- Do you contract with third parties that may **subcontract activities** to other foreign and domestic providers? – For what services?
- Do you use any **integrated technology** to automate vendor risk assessment and mitigation processes – Are you being efficient?
- Are your vendors familiar with **consumer financial protection laws** affecting your industry (e.g., unfair, deceptive, or abusive acts or practices)?
Audit Strategy: As 3rd party risk management is an enterprise risk, internal audit is in a unique situation to report on its sufficiency across the organization.

Leading Practice

1. Appoint a "central point of contact" (CPC) in internal audit to face off with 3rd party management similar to other enterprise risks
2. Set the audit standard for 3rd party audit programs
3. Serve as SME on 3rd party management within audit
4. Conduct reviews and identifies potential risks and required remediation
5. Influence/coach business and control functions audits
6. Develop a point of view on the overall design and operating effectiveness of vendor risk management procedures
7. Communicate and reports that point of view to management and the Chief Audit Executive
Independent Reviews

Independent reviews should be conducted on the third-party risk management process, particularly when a company involves third parties in **critical activities**. A review should consider the following:

- ensuring third-party relationships continue to align with the company's business strategy
- ensuring proper oversight and accountability for managing third-parties (e.g. roles and responsibilities clear, possess the requisite expertise, resources, and authority)
- ensuring appropriate staffing and expertise to perform due diligence and ongoing monitoring and management of third parties
- identifying and managing third party risks, including foreign-based third parties and subcontractors
- ability to report, track and mitigate identified material breaches, service disruptions, or other material issues.
- ensuring conflicts of interest or appearances of conflicts do not exist
- identifying and managing concentration risks that may arise from relying on a single third party for multiple activities
## Critical Success Factors

<table>
<thead>
<tr>
<th>Critical Success Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Comprehensive Inventory of TP</td>
<td>Maintain comprehensive inventory of third parties and the services they provide which is cleansed and available to the third party risk management team</td>
</tr>
<tr>
<td>2. Develop and maintain comprehensive catalog of third party risks</td>
<td>Understand the full complement of risks third parties can expose your firm. Maintain a master risk register tied to the issues that the regulators (e.g. Consumer Financial Protection Bureau, FDIC, Federal Reserve and OCC) are actively pursuing. Maintain map of critical services and what risks these services may cause</td>
</tr>
<tr>
<td>3. Provide a risk based segmentation of your third party services</td>
<td>Develop a standard risk tiering methodology and apply it consistently through out your company. Devote the most effort to services defined as critical to your company and consistently apply due diligence globally</td>
</tr>
<tr>
<td>4. Implement a rules-based due diligence process</td>
<td>Consistently put your third parties and services through a similar rules based risk process. Carefully design rules that will tier your vendor and drive what risk domain and due diligence and monitoring process is required</td>
</tr>
<tr>
<td>5. Employ a disciplined ownership, governance and escalation framework for your third party risk management</td>
<td>Ensure your company has a clear third party risk management owner and that group has the right authority and clear decision-making powers to develop the necessary process, organizational structure and technology needs for continuous improvement</td>
</tr>
<tr>
<td>6. Receive an independent assessment of your critical third party services</td>
<td>To ensure you have identified and assessed the most critical activities and regulatory impact consider receiving an independent assessment of your third party services and how your risk criticality compares to your peers</td>
</tr>
<tr>
<td>7. Create efficiency and accuracy through Integrated technology</td>
<td>to increase your efficiency and accuracy of your risk assessments: Purpose-built, off-the-shelf applications have matured over the last few years and may be the right answer for your third-party risk management needs. Building your own can be difficult.</td>
</tr>
<tr>
<td>8. TPRM Internal Audit lead</td>
<td>Identify an internal audit central point of contact (CPC) that understand is what the regulators are looking for, so you can find and address identify weaknesses before your examiners do</td>
</tr>
<tr>
<td>9. Streamline use of third parties</td>
<td>Company mergers, acquisitions and lack of corporate wide sourcing activities may have produced duplicate third parties and services and a rationalization initiative will not only save you money but lower your risk potential.</td>
</tr>
<tr>
<td>10. Organize three lines of 3rd party risk defense</td>
<td>Establish three lines of defense: 1) business owners — they own the risk and implement actions for risk identification and mitigation; 2) third-party oversight — they establish the policies and procedures, provide oversight for key risks, and identify opportunities for improvements as guidelines change; and 3) internal audit — they provide an independent, systematic and disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes</td>
</tr>
</tbody>
</table>
Summary

- **Plan and Identify** inherent risks associated with the third-party activity
- Perform the proper **due diligence and 3rd party selection**
- **Negotiate contracts** defining rights and responsibilities of all parties specific to your identified risks
- **Continually monitor** third parties' activities and performance – focus on critical activities
- **Terminate** 3rd party relationships if certain criteria are not met, have transitions plans ready
- Provide senior **Oversight and Monitoring**
- **Maintain proper** **Documentation and Reporting**
- **Conduct Independent Reviews** of the risk management process
Questions
Contact Information

Dennis Frio
FS National Director
Third Party Risk Practice Leader
T (direct) +1 646 825 8470
T (mobile) +1 973 747 2281
E dennis.frio@us.gt.com
W www.grantthornton.com

John Swanick
National Insurance Advisory Practice Leader
Business Advisory Services
Insurance Regulator Leader
T (direct) 215 814 4070
T (mobile) +610 246 2156
E John.Swanick@us.gt.com