Risk Management: IT Vendor Management and Outsourcing

October 6, 2015
Definitions

• **Third Party** is any entity not under direct business control of a given organization. Many people equate third parties with vendors, but that’s not always the case; consider:
  - Vendors/suppliers of products or services (Business Associates)
  - Business partners (JV partners, alliances, etc.)
  - Marketing partners
  - Strategic consultants
  - Government agencies
  - Regulatory bodies
  - Customers

• **Third Party risk management** encompasses vendor risk management, but is more broadly focused on gaining a understanding of organizational risks and understanding which of those risks may be either positively or negatively affected by third-parties.

• **Third Party inventory** is a comprehensive list of third parties from across the company.
Definitions (continued)

- **Third Party Risk Profile** is the combination of:
  - **Entity risk** – risk associated with the third-party organizational structure and characteristics (e.g. size/complexity, past experience, etc.)
  - **Service risk** – risk associated with the product or service provided (e.g. regulated data provided, availability requirements, etc.)

- **IT Vendors** add a significant amount of risk to any organization’s risk posture. For the purposes of managing IT Vendor Risk, and that of outsourcing in general, organizations must implement effective Third Party Risk Management programs.
Third Party Risk Management – Target operating model

The purpose of the target operating model is to define how the TPRM program will operate while taking into account regulatory guidance and industry leading practices, while maintaining alignment with the organization’s operational risk tolerances.

The Target Operating Model addresses the following:

1. Strategic planning for a TPRM Program in alignment with the enterprise and operational risk management
2. Target governance structure with clear roles & responsibilities
3. Program Management of the TPRM Program
4. Enterprise TPRM Policy and Procedures
5. Foundational practices and target state third party risk management life cycle stages that are focused at the right level so as to optimally identify, measure, report, and manage risk
   - Planning for the use of third parties
   - Initial due diligence of third parties
   - Contract negotiations with third parties
   - Ongoing monitoring, re-assessment, and oversight of the third party relationships
   - Disengagement of third parties
6. Technology and tools to operationalize and efficient and effective TPRM Program across the above life cycle stages
7. Periodic evaluation and updating of the TPRM target operating model
Trust but Verify – Vendor for Major Health Care Company
Alright, not so bad!
Trust but Verify - Continued
Trust but Verify – This Is Why!
Why are we discussing?

• $50bn estimated annual losses to business from data and identity theft
• Third Parties are a major source of data breaches of regulated data.
• 74% of companies do not have a complete inventory all third parties that handle personal data of its employees and customers¹
• 73% of companies lack incident response processes to report and manage breaches to third parties that handle data ¹
• Breaches and non-compliance can lead to significant impacts: brand, reputation, fines, lost revenue and/or regulatory sanctions
• Companies often face direct financial impacts: investigations, legal fees, credit monitoring services for victims, reissuance of credit cards, government fines, consent decrees and other regulatory sanctions

¹PwC 2014 Global State of Information Security Survey
Regulatory Drivers

Regulatory considerations

In the last 10-15 years, multiple new regulations in all industries have demanded increased focus on how organizations monitor security and privacy practices of their third parties.
The Financial Industry is often 5-7 years ahead of other industries. This OCC bulletin sets the following expectations for supervised entities (banks) and provides a good example of what should be included in an effective TPRM program.

**OCC 2013-29 Expectations**

- A bank should adopt **risk management processes** commensurate with the level of risk and complexity of its third-party relationships.
- A bank should ensure **comprehensive risk management and oversight** of third-party relationships involving critical activities.
- An **effective risk management process throughout the life cycle** of the relationship includes:
  - Plans that outline the bank’s strategy, identify the **inherent risks** of the activity, and detail how the bank **selects, assesses, and oversees** the third party.
  - Proper **due diligence** in selecting a third party.
  - **Written contracts** that outline the rights and responsibilities of all parties.
  - **Ongoing monitoring** of the third party’s activities and performance.
  - **Contingency plans for terminating** the relationship in an effective manner.
  - Clear **roles and responsibilities for overseeing and managing** the relationship and risk management process.
  - **Documentation and reporting** that facilitates **oversight, accountability, monitoring, and risk management**.
  - **Independent reviews** that allow bank management to determine that the bank’s process aligns with its strategy and effectively manages risks.
Sample headiness involving third parties

The hackers who stole 40 million credit and debit card numbers from a large discount retailer appear to have breached the discounter’s system by using credentials stolen from a vendor.  
– Wall Street Journal, January 2014

Hackers successfully stole prepaid debit card information from the Indian and US-based third-party vendors of several large multi-national credit card institutions, fraudulently withdrawing $45M from ATMs worldwide.  
– Wall Street Journal, May 2013

17,300 patients have their protected health information breached following a scam executed by a group posing as a vendor.  
– Modern Healthcare, May 2013

What a vendor got wrong: The risky business of hiring from competitors
A vendor hiring the former CEO of its client’s largest competitor, to lead its company. Despite a decades-long relationship, the client terminated its contract with the vendor due to this hiring decision.  
– Modern Healthcare, May 2013

FTC Data Security Settlement Highlights Need for Third-Party Vendor Management and Oversight
Federal Trade Commission (FTC) announced a settlement with a translation services providers following the public exposure of thousands of medical transcript files containing personal medical information.  
– HL Chronicle of Data Protection, January 2014

A bank points outage finger at its technology provider
A bank says a failure on its technology provider’s part to correctly fix an identified instability within the bank’s storage system led to the seven-hour service outage last week.  
– By Eileen Yu, ZDNet Asia on July 14, 2010

'We Blew It': A world leader in consumer retail goods Admits to Mistakes Over Child Labor
A multi-billion dollar sportswear company admitted yesterday that it “blew it” by employing children in Third World countries but added that ending the practice might be difficult.  
– Steve Boggan Independent/UK Oct 20, 2001

Breach at a large merchant processor cost approximately $94 million and removal from the global registry of a major card issuer.  
– CNN, March 2012

3.6 million personal income tax returns and 657,000 business filings exposed due to third party data breach.  
– Washington Post, October 2012

Foreclosure defense lawyer is missing; his law partner says at least $6M in firm money is gone
A foreclosure defense lawyer in Florida has been reported missing as authorities investigate the reported disappearance of at least $6 million in funds held by his law firm in trust accounts.  
– Criminal Justice Apr. 15, 2013

Investigators said that for years, high-ranking executives at the company’s China operations used travel agencies as money-laundering shops to funnel bribes to government officials.  
– New York Times, July 2013

Recent Ponemon Institute surveys reveal:
• Unsecure third parties including cloud providers are seen as one of the top three threats to an organization
• 41% of the companies surveyed experienced a data breach caused by a third party. And the consequent loss of brand value typically ranged from $184 million to more than $330 million
Business Drivers

Globalization continues and business partnerships are increasingly being leveraged as strategic enablers.

According to PwC’s 14th Annual Global CEO Survey:
• Companies are reshaping strategies and operating models—focusing on innovation, collaboration, and talent—to find new sources of revenue growth and competitive advantage

Partnership will be key
• 40% of CEOs expect the majority of innovations over the next three years to be co-developed with partners
• 50% said their companies will enter into a strategic alliance or JV in the coming year

• Roughly a third of CEOs indicated their companies plan to complete a cross-border merger or acquisition, or outsource a business process or function in the next year

• As organizational models shift and risk profiles evolve, executives and Boards seek greater transparency and increased assurance that the company’s most significant risks are appropriately mitigated
Inventory third parties – A multi-faceted approach

1. Existing Inventories
2. Review Contracts
3. Analyze Accounts Payable
4. Business Questionnaire
5. Conduct Meetings

Profile Against Defined Risks
Analyze & Categorize Determine Assessment Type
Perform Self-Assessment, Desktop Review or On-site Assessment

Develop Inventory

Design Assessment Strategy

Execute Strategy

Review Risks Against Assessment Results

October 6, 2015
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.

**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.

**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.
Profile third parties – Define risk components

Third Party Risk Profile

### Entity Profile
- Experience & size etc. (20%)
- Familiarity with Company (Includes contract status) (40%)
- Prior Reviews (40%)

### Service Profile
- Data & Information
  - Data Sensitivity (20%)
  - Availability Impact (10%)
  - Uptime Req. (5%)
- Service Type (15%)
- Service Scope (15%)
- Service Operation

### Regulatory/Legal
- SOX
- GxP
- PCI
- HIPAA (25%)

<table>
<thead>
<tr>
<th>Category</th>
<th>Weighting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experience &amp; size etc.</td>
<td>(20%)</td>
</tr>
<tr>
<td>Familiarity with Company</td>
<td>(40%)</td>
</tr>
<tr>
<td>Prior Reviews</td>
<td>(40%)</td>
</tr>
<tr>
<td>Data &amp; Information</td>
<td></td>
</tr>
<tr>
<td>Service Type</td>
<td>(15%)</td>
</tr>
<tr>
<td>Service Scope</td>
<td>(15%)</td>
</tr>
<tr>
<td>Service Operation</td>
<td></td>
</tr>
<tr>
<td>Regulatory/Legal</td>
<td></td>
</tr>
<tr>
<td>SOX</td>
<td>(25%)</td>
</tr>
<tr>
<td>GxP</td>
<td></td>
</tr>
<tr>
<td>PCI</td>
<td></td>
</tr>
<tr>
<td>HIPAA</td>
<td></td>
</tr>
</tbody>
</table>

October 6, 2015
**Profile third parties – Narrow the focus**

- Total Third Party inventory
- Remove categories that don’t pose risk
- Apply weightings to derive overall risk profile score
- Prioritize higher risk Third Parties

- Entity Risk
- Service Risk

- On-site assessment
- Desktop review
- Self assessment

**17 October 6, 2015**
Develop an efficient assessment approach

Third Party Risk Profile

Self Assessment
• Third party responds to questionnaire
• Least resource intensive

Desktop Review
• Off-site assessment consisting of interviews and limited document review
• Conducted using any-shore model

On-site assessment
• On-site assessment consisting of interviews and document review
• Most resource intensive

Risk & Complexity
Resources Required
Comfort Obtained
Develop an efficient assessment approach (continued)
# Example – Third party performance scorecard

## Third Party Performance Scorecard

<table>
<thead>
<tr>
<th>Category</th>
<th>Metric</th>
<th>Far Below</th>
<th>Below Expectations</th>
<th>Meets Expectations</th>
<th>Exceeds Expectations</th>
<th>Far Exceeds Expectations</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality Assurance Program</td>
<td>Firm’s quality objectives are formally documented</td>
<td></td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Method of assuring quality is defined</td>
<td></td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Defined quality unit is independent from manufacturing and/or development</td>
<td></td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>0.00</td>
</tr>
<tr>
<td>Security</td>
<td>Employee and visitor access to the facility is documented in a written policy</td>
<td></td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Levels of access to the facility is documented and a current listing of users with access is maintained</td>
<td></td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Removal of company and/or customer assets is documented</td>
<td></td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>0.00</td>
</tr>
<tr>
<td>Software Development Methodology</td>
<td>Formal methodology is followed for software developments and enhancement projects</td>
<td></td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Planning activities are documented and endorsed by management</td>
<td></td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Quality inspects project deliverables to ensure adherence to the plan</td>
<td></td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>0.00</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>Procedures for reconstructing the network infrastructure are documented and have been tested</td>
<td></td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Storage area is protected from natural events, theft, and security intrusion</td>
<td></td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Recovery procedures are documented for unplanned outages</td>
<td></td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>□</td>
<td>0.00</td>
</tr>
</tbody>
</table>
Track, report and respond to assessment results

1. Profile

- Third Party Data Collection
  - Business Sponsor
  - Previous Assessments
  - Third party contacts
  - Contracts

Preliminary Entity Profiling

Preliminary Service Profiling

2. Assess

Preliminary Third Party Rating

Output:
- Assessment Type
- Assessment Scope

Third Party Processes and Controls

Technical Security Assessment

Assessment Report

Third Party Report

3. Review and Decide

Residual Risk Rating and Score

Business Action:
- Accept
- Share/Transfer
- Reduce

Remediation and Re-assessment

Periodic Review

October 6, 2015

PwC
The Internal Audit group has key responsibilities as part of the third line of defense to ensure the TPRM Program is operating efficiently.

**Internal Audit**
- IA needs to 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. This may be done for a small number of Third Parties during the early deployment phase of the organizations TPRM Program, and is typically not part of ongoing operations.
- This should occur in the early establishment of the Program and taper off as the Program matures and assurance is gained that the on-site visit process is working as designed.
- As part of the TPRM Program’s second line of defense, a central TPRM Office is usually responsible for ensuring that the ongoing operational aspects of the Program are reviewed and monitored on a ongoing basis to validate that key stakeholders are performing their roles effectively – this includes how third party managers and SMSs perform third party on-site activities.
- IA’s focus is typically on the more significant relationships from an inherent and residual risk perspective based on the 2nd line of defense’s risk assessments.
- IA being the 3rd line of defense, should not be influenced by what TPRM or Subject Matter Specialists may have done during their on-site visit.
- IA should focus on the third party on-site activities of what the TPRM Program requires. Not all areas need be assessed during each audit. If several third parties are to be visited, then the review of activities may be split between a number of third parties.
- Consideration regarding who owns the controls should also drive the need for IA to audit TPRM (i.e., where controls are owned by the company and operated by the third party, less risk exists) as well as any compensating controls that may exist within the organization to help mitigate risks associated with the third party’s practices.
Questions & contact information

John Maynor
Director, Cybersecurity & Privacy
john.d.maynor@pwc.com
(937)469-3042
Not for further distribution without the permission of PwC.

These materials are for general information purposes only, and are provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose.

The information contained in this document is shared as a matter of courtesy and for information or interest only. PwC has exercised reasonable professional care and diligence in the collection, processing, and reporting of this information. However, data used may be from third-party sources and PwC has not independently verified, validated, or audited such data. PwC does not warrant or assume any legal liability or responsibility for the accuracy, adequacy, completeness, availability and/or usefulness of any data, information, product, or process disclosed in this document; and is not responsible for any errors or omissions or for the results obtained from the use of such information. PwC gives no express or implied warranties, including, but not limited to, warranties or merchantability or fitness for a particular purpose or use. In no event shall PwC be liable for any indirect, special, or consequential damages in connection with use of this document or its content. Information presented herein by a third party is not authored, edited or reviewed by PwC and PwC is not endorsing third parties or their views. Reproduction of this document or recording of its presentation, in whole or in part, in any form, is prohibited except with the prior written permission of PwC. Before making any decision or taking any action, you should consult a competent professional adviser.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2015 PricewaterhouseCoopers LLP. All rights reserved. PwC refers to the United States member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.