Third Party Risk Continuum

Kirt Seale
National Special Attestation Report Solution Leader
Grant Thornton LLP

January 10, 2014
Biography

- **Kirt Seale: National Special Attestation Report Solution Leader for Grant Thornton LLP**
  - Responsible for understanding the professional standards relating to Service Organization Control (SOC\textsuperscript{SM}) reports and the related Attestation Standards and developing technical firm guidance to be applied by Grant Thornton professionals.
  - Oversees the development of policies, practice aids, and training as part of a quality assurance program relating to the delivery of these services.
  - Through his work on nearly sixty SOC projects annually, he monitors how service organizations are gaining real business value from the completion of these types of audits.
  - Experience in delivering SOC audit services in a variety of service organizations, including those that provide accounting, securities settlement, trust administration, payroll processing, data center hosting, software as a service, and lockbox services.
  - Worked within a variety of industries, but specializes in the technology and financial services/financial institutions industries.
Learning objectives

- Understand fundamental third party risk assessment activities
- Identify various projects/services that may be used to assess third party risk
- Identify framework for selecting the right type of project for your needs
Issues of the day

- Increased regulations
- Increase in outsourcing relationships
- Complexities within assurance services available
- Changes may lead to confusion
- More options = getting the right report
Agenda

• **Current trends and third-party risk considerations**
• Third party risk continuum
• Risk mitigation/assurance options
• Selecting the right level of assurance for your organization
Current trends

In today's environment, the responsibility for risk mitigation rests within the organization itself; the risk cannot be outsourced.

What do you know about these organizations:

• ClearForest
• Global Payments
• Advanced Data Processing
• Portal Healthcare Solutions LLC
What's a third party?

Third parties are businesses that are not under direct business control of the organization that engages them.

This may include:

- Vendors
- Distributors
- Suppliers
- Franchisees/licensees
- Joint venture or alliance partners
- Technology outsourcing providers
Why is third-party risk important?
Industries with highest risks

- Government
- Healthcare
- Banking
- Investment/fund managers
- Payroll management companies
- Financial Services
Defining the third-party universe

- Analyze comprehensive vendor listing (A/P master file, legal, procurement)
- Exclude the following:
  - Maintenance, repair, operations vendors
  - Providers of raw materials or finished goods
- Confer with in-house legal resources
  - Additional source of data
  - Contractual details will be helpful
- Consider other departments that may need to be consulted
Responsibility for third-party risk management
Where do you begin?

Project objective

• **Risk assessment and appeals processes**
  – Customize the vendor due diligence process depending on the company’s specific risks
  – Rule-based point values assigned
  – Cumulative score will dictate level of additional investigation if required
## Factors to consider when assessing risk

<table>
<thead>
<tr>
<th>Risk domain</th>
<th>Assessment factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>• Level of importance of vendor to corporate operations</td>
</tr>
<tr>
<td>Reputational</td>
<td>• Magnitude of potential loss if there are problems with the vendor relationship</td>
</tr>
<tr>
<td>Regulatory</td>
<td>• Level of vendor oversight/monitoring</td>
</tr>
<tr>
<td></td>
<td>• Reporting required by outside regulatory body</td>
</tr>
</tbody>
</table>
Factors to consider when assessing risk

<table>
<thead>
<tr>
<th>Risk domain</th>
<th>Assessment factors</th>
</tr>
</thead>
</table>
| Operational   | • Type of vendor – nature of products/services provided  
|               | • Frequency of communication with vendor                                            |
| Financial     | • Annual spend with vendor                                                          |
| Compliance    | • Current safeguards or controls design to ensure compliance with relevant regulations  
|               | • Availability of audit reports or existence of "right to audit" clause             |
Needs analysis approach

High, medium or low-risk areas are determined based on the risk factors:

- Strategic importance
- Business operations risk
- Legal/regulatory compliance
- System reliance and capability
- Fraud risk
- External factors
- Human capital risk
The needs analysis starts with the owner of the risk.
The determination of the level of assurance dictates the nature of the report/certification required.
The determination of the level of assurance dictates the nature of the report/certification required.
Agenda

- Current trends and third-party risk considerations
- **Third party risk continuum**
- Risk mitigation/assurance options
- Selecting the right level of assurance for your organization
Third party continuum

- **Vendor questionnaire**: Low effort/low assurance
- **Shared assessment**: Low effort/moderate assurance
- **ISO**: Moderate effort/low to moderate assurance
- **Internal audit vendor review**: Moderate effort/moderate assurance
- **SOC 1, 2, 3**: High effort/high assurance
Agenda

• Current trends and third-party risk considerations
• Third party risk continuum
• Risk mitigation/assurance options
• Selecting the right level of assurance for your organization
Risk mitigation techniques

- Transaction monitoring
- Increased data analysis and reporting
- Contract renegotiation
- Independent reviews
- Audits
- Site visits
- Questionnaire
## Self assessments/questionnaires

<table>
<thead>
<tr>
<th>Service description</th>
<th>A standard, internally generated questionnaire focused on a consistent set of questions inquiring about certain controls and safeguards. Then you would evaluate responses and, ideally, escalate issues if deficiencies or other concerns regarding the vendor were identified.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pro</strong></td>
<td>A simple, low-cost, internally generated questionnaire can focus on only those areas of concern for your organization.</td>
</tr>
<tr>
<td><strong>Con</strong></td>
<td>Information and responses provided are not verified by an external party, so the level of assurance the completed questionnaire provides is low.</td>
</tr>
</tbody>
</table>
## Compliance with standards

<table>
<thead>
<tr>
<th>Service description</th>
<th>A national or international standards setting body defines the requirements.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pro</strong></td>
<td>National or global standard that may be widely accepted. Good visibility into the standard that has been met.</td>
</tr>
<tr>
<td><strong>Con</strong></td>
<td>The criteria met may not be those critical to your organization. These certifications do not include an explanation of the auditor's work and procedures.</td>
</tr>
</tbody>
</table>
### Internal Audit – Vendor review

<table>
<thead>
<tr>
<th>Service description</th>
<th>Tailored vendor review that is developed as part of the Internal Audit plan and therefore is focused on the key risks relating to the relationship.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pro</strong></td>
<td>Highly customized. Independent assessment performed by those that understand your environment and risks very well. Good visibility into procedures performed and evidence obtained.</td>
</tr>
<tr>
<td><strong>Con</strong></td>
<td>Both the internal and external cost is the responsibility of your organization. Some contracts may not include a &quot;right to audit clause.&quot;</td>
</tr>
</tbody>
</table>
## Attestation reports

<table>
<thead>
<tr>
<th>Service description</th>
<th>Standard externally generated reports focused on criteria that are, or can be, communicated to all readers/users of the report. Then you would evaluate responses and, ideally, escalate issues if deficiencies or other concerns regarding the vendor were identified.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pro</strong></td>
<td>High level of assurance as management and an independent auditor provide an opinion regarding the services and controls of the third party. Detailed testing activities typically included.</td>
</tr>
<tr>
<td><strong>Con</strong></td>
<td>Designed to meet the requirements of a common set of services and controls, so it may not include every aspect of the services you are interested in.</td>
</tr>
</tbody>
</table>
## Use of attestation reports

<table>
<thead>
<tr>
<th>SOC 1</th>
<th>SOC 2</th>
<th>AT 101</th>
</tr>
</thead>
</table>
| • Provides a vehicle for reporting on a service organization’s system of internal control relevant to a user organization’s internal control over financial reporting.  
• Intended as auditor-to-auditor communication, with specific content dependent on the service organization’s system. | • Addresses controls pertinent to the Trust Services Principles of security, availability, processing integrity, confidentiality and privacy.  
• Includes many of the same elements as a SOC 1 report.  
• Principles and criteria developed by the AICPA and the Canadian Institute of Chartered Accountants. | • Allows service organizations to provide user organizations and other stakeholders with a tailored report on controls that are relevant to the services.  
• Highly flexible and can be leveraged for multiple industry standards (e.g., NIST, ISO). |
Consider the following when reviewing a SOC report:

• Time period covered
• Handling of subservice providers (carve-out vs. inclusive)
• In-scope and out-of-scope locations
• Construction of control objective and control activities
• Sampling and testing methodology
• Exceptions noted and management response
Agenda

- Current trends and third-party risk considerations
- Third party risk continuum
- Risk mitigation/assurance options
- Selecting the right level of assurance for your organization
Selecting the "right" level of assurance

• Take into account the risk factors that surfaced during the risk assessment.
• Consider the culture, structure, people and processes of your organization.
• What type of industry or market do you operate in?
• How does your organization leverage vendors to be more competitive in the marketplace, and what is the regulatory environment in which you operate?
• Who will bear the costs involved?
Questions?
Disclaimer

This Grant Thornton LLP presentation is not a comprehensive analysis of the subject matters covered and may include proposed guidance that is subject to change before it is issued in final form. All relevant facts and circumstances, including the pertinent authoritative literature, need to be considered to arrive at conclusions that comply with matters addressed in this presentation. The views and interpretations expressed in the presentation are those of the presenters and the presentation is not intended to provide accounting or other advice or guidance with respect to the matters covered.

For additional information on matters covered in this presentation, contact your Grant Thornton LLP adviser.
Thank you for attending

Visit us online at:

www.GrantThornton.com

twitter.com/GrantThorntonUS

linkd.in/GrantThorntonUS