Risk Rating Third Parties: Optimizing Risk Management Outcomes
ABSTRACT

Risk rating of third party providers is an essential aspect of a comprehensive risk management program. When risk rating is based on pre-determined criteria, outsourcers can use that rating on an objective basis for identifying actual-versus-perceived risk, and for comparing third parties from a risk perspective related to specific risk areas, such as financial health, security controls and resiliency.

This objectivity informs a more effective evaluation of a third party's ability to maintain a control profile that better mirrors the expectations of the outsourcing organization.

This paper discusses:

• What third party risk rating is;
• Why risk rating is needed; and
• How an organization can apply risk rating best practices as part of their risk management program.

A formal risk rating process will determine assessment cadence and enables and prioritizes the assessment depth and specific actions for those assessments. To be effective, risk rating must be based on documented parameters, which include scoring against the defined risk tolerance and risk appetite statement of the outsourcer. It is essential that a pre-engagement risk rating is performed on every potential third party to determine appropriate levels of due diligence oversight and set relevant expectations for ongoing assessments.

Taking this approach allows stakeholders, including risk managers, senior executives and board members, to focus and apply appropriate resources to third party oversight. This, in turn, enables the organization to be more effective in:

• Assigning the timing and frequency of ongoing risk management activity;
• Determining the need for and allocation of resources to reassessment; and
• Achieving better overall risk management outcomes.

Benefits of establishing a well-structured, comprehensive rating process include: focused organizational support for internal and external critical risk functions; identification of significant gaps in due diligence and control processes; and the opportunity to make control assessment processes more cost effective and efficient.
**ISSUE LANDSCAPE**

While risk rating of vendors can be performed at any time during the third party risk management (TPRM) lifecycle, it must be used in the pre-assessment phase to determine the level of risk and corresponding depth of assessment that will be required, based on the type of services and the risk posed by the individual provider.

Risk rating, at any point in the lifecycle, is done against a set of documented risk rating parameters that are tied to the outsourcer’s risk appetite and relevant key risk indicators.

This paper serves as a basic, best practices guideline for risk rating. A methodology is outlined for assigning an initial pre-engagement risk rating, based on the inherent and residual levels of risk that a specific third party might pose to the outsourcing organization.

Only when the controls criteria for each risk type have been examined at the inherent risk level can target risk can be examined at the individual provider level to determine which risks can be transferred, controlled or otherwise mitigated. The remaining level of risk constitutes the residual risk which should correspond to the organization’s pre-determined risk tolerance and risk appetite statement.

---

**Key Components of a Risk Rating Process**

Fundamental, best practices components are presented below which outsourcers can tailor to suit their specific needs. For the purposes of this paper, the following definitions are used.

**Definition of Third Party Risk Rating**

A standardized, scalable and repeatable due diligence procedure for identifying risks and categorizing third party providers in light of those risks.

The best practices process for risk rating is:

1. Identifying the inherent risk of each outsourced activity;
2. Defining risk rating by activity type;
3. Establishing controls criteria;
4. Compiling a third party and services inventory; and
5. Applying risk ratings to individual third parties.

**Definition of Risk Prioritization Scoring Method**

A systematic approach that quantifies risk in terms of loss potential, then sequences individual risks to determine the order in which additional and/or compensating controls should be implemented.

While the process of risk rating can be standardized, the rating applied to any given third party is unique to the outsourcer’s risk tolerance for a specific activity. Risk tolerances are set as a function of an organization’s risk appetite; that is, the amount of risk an organization will accept in pursuit of its business goals.

Defining, documenting and communicating the risk appetite statement is part of a well-developed risk management framework. Risk appetite statements typically include several layers of risk tolerance expression, vertically structured to be relevant from the board to the business unit level. Business unit level expressions of risk tolerance set the context for third party risk management.

An in-depth understanding of the inherent risk associated with each activity and the importance of that risk within the outsourcer’s environment are essential to gaining a better understanding of the degree of assurance required for any given third party relationship.

Activities that carry high inherent risk, combined with low risk tolerance, require higher levels of assurance. Those deemed critical to an organization’s business resiliency would carry the highest priority for assessment.

Some third parties present minor risk exposure, while others can expose an outsourcer to substantial risk. As demonstrated in Figure 1, risks exist at two levels:

1. The outsourcer exposure level; and
2. The service level.

---

The increasing severity of consequences for regulatory violations by vendors in complex global supply chains is matched only by the corresponding damage to reputation when vendor network violations get exposed. The growing volume and widening range of global transactions in global geographic barriers and amplified company exposure to issues that were once considered distant threats. Not only are companies at risk, but also, increasingly, leadership and board members are being held accountable for their companies’ supply-chain-related regulatory breaches.

Needle in the haystack: Monitoring vendor networks through supply chain analytics

PwC
BEST PRACTICES METHODOLOGY GUIDELINES

Identifying Inherent Risk of Each Outsourced Activity

In order to establish the requirements and the resulting controls necessary to manage outsourced activities the risks presented by those activities must first be determined.

Identifying the inherent risk of specific activities and setting control and assessment criteria on this basis allows all third parties to be assessed against a uniform set of requirements based on the risk that the third party’s activity presents. The determination of risk by activity should occur before an assessment of a given provider takes place.

Best practice for identifying and rating inherent risk is:

• Establishing the inherent risk of outsourcing these activities;
• Linking the risk to a baseline metric for comparison and priority such as financial impact;
• Defining potential third party exposure, without regard to an individual provider; and
• Determining the residual risk that remains after controls are in place at the individual provider level.

By defining and standardizing a rating for inherent risks, it is possible to evaluate and establish procedures for managing each risk, as shown in Figure 2. Once these are established, an outsourcer can follow internal guidelines for determining the level of a pre-engagement assessment and establish frequency and level of subsequent re-assessments.

Defining Risk Rating Scale by Activity Type

An appropriate risk rating process will define specific categories and criteria that can be used to produce an objective score based on known provider information and rate that on a scale such as high, medium or low.

Outsourcers should determine the categories and criteria based on their own unique risk tolerance for activities and types of services, as well as the materiality of a given third party. Establishing a risk appetite framework that is communicated effectively at all levels within an organization is a best practices prerequisite to establishing a coherent risk culture that optimizes third party risk mitigation performance.

Table 1 provides a non-exhaustive list of risk rating parameters, which outsourcers should expand upon based on their own risk tolerance and service scope priorities.
Once an outsourcer has determined the factors that contribute to the risk of a particular outsourced activity, rating classifications can be established that are aligned with the controls that will best manage these risks. This classification process allows an assessment to be scoped based on the actual risk that the specific activity and provider present to the outsourcer.

Failing to properly scope and define third party assessments generally results in assessments that may be:

• Overly broad, creating inefficient use of resources for both the third party and the outsourcer.
• Unable to effectively measure and manage outsourced risk.
• Unable to drive proactive corrective actions for planning and mitigation.

Classification of the services by inherent risk is an important step in understanding and assigning a risk rating to a specific third party. This inherent risk classification is a key indicator of the material effect a particular third party may have on the business due to a financial condition limiting the third party’s ability to mitigate a security, availability or other service delivery issue. Determining this material effect early in the risk rating process is an important step in understanding the subset of third parties that represent the greatest, operational risk to the organization.

The following are key to developing a process to establish risk ratings based on specific requirements and criteria:

• Providing an opportunity for all stakeholders from IT, Procurement, Legal, Disaster Recovery, and business units to provide appropriate input to ensure that all issues/concerns across the organization are taken into account.
• Setting risk rating criteria that:
  o Take into consideration generally accepted risk management criteria. See Table 2 for a list of frequently applied key risk rating areas.
  o Is forward-facing, where possible, to consider emerging risks.
  o Establishes ratings with scoring/weighting factors that correlate to a high/medium/low risk level or a numerical scale.
  o Utilizes key rating components to include, but not be limited to, those listed in Table 3.
• Standardizing and formalizing the risk rating process to:
  o Ensure consistent application to and validation of all new and existing providers, for both due diligence and repeat assessments.
  o Define consistent format and rating scales, to facilitate transparency and communication.
  o Produce a risk rating document that is included in a formal and defensible third party assessment package that can be used to support audit and regulatory reviews.
• Assigning to each third party one or more risk ratings (where multiple services are provided) and consider an overall relationship risk rating as the basis of assessment and other oversight activities.
• Providing periodic, documented awareness training to employees, procurement and third parties with clear, consistent information and messaging, to increase awareness of risk management goals and policies. This can include professional development for risk managers, to establish a stronger standard that incorporates security and risk management training in all third party risk and procurement processes.

The remaining risk rating steps will further determine the actual risk rating assigned to a particular third party and the level of effort required for the overall assessment process.

### Establishing Controls Criteria

A primary purpose of creating risk categories is to better manage each of the defined risk categories by facilitating the development of a standardized set of risk controls and related assessment requirements.

Outsourcers can define key control indicators (KCIs) that more clearly identify and quantify their own third party risk exposure. These metrics can be used to demonstrate how well they are managing against their own stated goals (and regulatory requirements). See Table 3 for examples of impact areas for KCIs.

### Compiling a Third Party Providers/Services Inventory

A complete and accurate third party (providers and services) inventory is a key requirement of the risk rating process and an important foundational requirement for the execution of a sound assessment process.

Since the assessment process is built on the ability to know and understand the third party and associated services landscape, the time and effort to build and maintain this inventory is critical to assessment program success. Maintaining an inventory also allows visibility into the types of third parties in use, as well as which ones can be eliminated or tagged as out of scope based on the outsourcer’s risk posture or other determining factors.

Once established, the following repeatable process for identifying and categorizing third parties can continue to be used when additional third parties are brought on board, and may be refined for quality improvement as needs change and experience dictates.

### Table 1: Suggested Categories and Criteria for Risk Rating

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>CRITERIA</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Type</td>
<td>Classification of data based on current policy defines scoped data that may have varying degrees of security/privacy requirements.</td>
</tr>
<tr>
<td></td>
<td>Location</td>
<td>Where data is accessed or transferred relative to the risk of a specific data classification, as well as any applicable regulations.</td>
</tr>
<tr>
<td></td>
<td>Transmission</td>
<td>How data is moved or migrated as part of services provided. May tie to locations relative to applicable regulation or other risk factors.</td>
</tr>
<tr>
<td></td>
<td>Connectivity</td>
<td>Specific connectivity to the third party and whether appropriate security controls are needed or present based on scoped data and location.</td>
</tr>
<tr>
<td></td>
<td>Remote Access</td>
<td>Requirement for remote access and whether appropriate security controls are needed or present.</td>
</tr>
<tr>
<td>Systems Access</td>
<td>System to System</td>
<td>System access that requires two systems/applications to be configured for data transfer with appropriate security controls and management approvals.</td>
</tr>
<tr>
<td>Availability</td>
<td>Impact on Operations</td>
<td>Impact on business operations due to an availability issue with the third party. This includes the ability to continue internal operations as well as provide services and products to customers.</td>
</tr>
<tr>
<td></td>
<td>Impact on Revenue</td>
<td>Impact on outsourcer, such as to revenue due to an availability issue with the third party.</td>
</tr>
<tr>
<td></td>
<td>Impact on Regulatory Guidance</td>
<td>Impact on the outsourcer’s ability to maintain compliance with applicable regulatory requirements due to an availability issue with the third party.</td>
</tr>
</tbody>
</table>

Having specified control criteria allows for:

• Tying a specific rating to assurance levels for the due diligence process as well as assignment of ongoing levels of oversight for each third party.
• Defining roles and responsibilities for the full lifecycle of the relationship.
• Developing contract templates that include review of risk rating for each third party against the established set of criteria and assignment of pertinent service level agreements (SLAs), key performance indicators (KPIs), key risk indicators (KRI), key control indicators (KCI), level of assessment, assessment cadence, whether an onsite is required and other relevant requirements based on the rating level assigned to the activity and relationship type.

The application of KCIs will substantially reduce assessment process frequency and scoping as the due diligence level for third parties will already be established (based on previously defined risk factors and risk control requirements).
Key best practices for identification and categorization include:

- Obtaining lists of existing third parties from all appropriate sources (Accounts Payable, Contracts, business units, Procurement, etc.).
- Cataloging all third party providers to establish a complete inventory, noting the services provided by each provider and if each provider has previously been rated and, if available, the rating achieved:
  - Identifying the Business Unit contact (identified/defined relationship owner) for the third party.
  - Identifying the third party contact.
  - Identifying whether third party is a public company or private entity.
  - Defining how the third party will be used within the outsourcing enterprise and set priorities for re-rating any previously rated provider based on any changes to the relationship or the outsourcer’s risk appetite.
- Complete with necessary data elements:
  - Data elements should include, but not be limited to, the following: third party name; physical location(s); key personnel, services provided; risk ratings, business owner, key contract dates, system/application usage; data classification; and data access requirements. The inventory should also include the general business vetting indicators that will be assessed. This vetting list may include, but is not limited to: financial viability, reputation, appropriate references, licensing requirements, insurance coverage, past/existing judgments or sanctions, regulatory and compliance requirements specific to the relationship (such as HIPAA, PCI, or others).

Key sources for inventory data include: business units, Accounts Payable, Contracts Management and Procurement departments. Outsourcers that have never built a complete and accurate inventory of existing third parties should consider starting with Accounts Payable, as existing third parties under contract should have one or more entries in the Accounts Payable ledger. Larger organizations tend to have a significant Procurement pipeline to show new as well as renewing third party relationships. However, that should not be relied upon, as Contracts Management and Procurement may be at some stage of negotiation or on-boarding and have not received a payment, meaning those vendors would be lacking in their list of approved vendors.

Applying Risk Ratings to Individual Third Parties
Once an outsourcer has completed the process of defining risk ratings and establishing assessment criteria for those ratings, each third party can be objectively and consistently rated against the established criteria.

As previously noted, the assignment of ratings to individual third parties requires an accurate and up to date inventory of all third parties. This application of risk rating results in a structured view of the outsourcer’s overall risk exposure from inventoried third parties at the pre-assessment stage of the lifecycle. Formal third party pre-assessment risk and ongoing assessment measures can then be executed and effectively reported.

It is important to note that third party risk ratings should be re-evaluated each time the provider is assessed to ensure that changes to services over time are included in any new assessments. In addition, the manner in which a third party performs their services may change (for example, a third party may subcontract a portion of their services). Thus, it is essential to make sure that a provider is still in the appropriate risk classification prior to executing the next assessment.

BENEFITS
The benefits of establishing a well-structured, comprehensive rating process include: focused organizational support for critical risk functions being outsourced; identification of significant gaps in due diligence and control processes; and the opportunity to make control assessment processes more cost effective and efficient.

Cost efficiencies can be expected to result from lower risk of reputational damage, improvements in compliance and efficient use of assessment resources. Risk rating is the most effective way for:

- Establishing the level at which a third party provider’s risk profile stance mirrors that of the outsourcing organization; and
- Monitoring that risk profile, to ensure it remains appropriate to the unique risks that third parties presents to the outsourcer, such as cyber and business resiliency risks.
Enterprise investment in a standardized and repeatable pre-engagement risk rating approach for all third parties can assist in:

- Highlighting significant gaps in pre-engagement due diligence processes.
- Enhancing transparency with internal and external stakeholders.
- Providing the opportunity to make processes more cost effective and efficient.
- Creating a structured and objective process for comparing the control posture of third parties.
- Increasing awareness of actual risk compared to perceived risk.
- Providing the basis for a more appropriately applied ongoing/continuous monitoring program.
- Providing a scale for third parties that provide differing services to be ranked and prioritized on a common basis.
- Promoting a proactive approach to mitigate risk.

**CONCLUSION**

A formal risk rating process allows assignment of risk in alignment with the overall organizational risk posture and provides a documented and defensible approach to assigning assessment resources and defining the level of oversight that needs to be applied to a particular third party provider.

A well-designed third party risk rating process is a key component of a comprehensive overall third party risk management program. Third party risk management program metrics that are derived through the risk rating process are the basis of reporting to senior management and the board of directors on the effectiveness and success of the program.

This type of rating, using objective risk factors, can help avoid disruptions from a third party, which may carry high impacts to an organization including: operating performance, direct financial cost, diversion or addition of resources and failure to support expected service delivery and/or risk management outcomes. The risk-based application of assessment methodology and resources can also set the stage for effective allocation of resources as the organization’s third party risk management program expands and matures.

---

1. Organizations within this paper are defined as: Outsourcer – the entity delegating a function to a subcontractor; Third Party – the subcontractor, by contract or otherwise, for the outsourcer; Fourth Party – a subcontractor to the outsourcer’s third party, regardless of whether the fourth party has a potential materiality/criticality impact on the original outsourcer.
2. Inherent risk is the risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls). [Source: ISACA Glossary. ISACA. 2017.] Residual risk is a calculation of the risk that remains after mitigating controls have been applied. [Source: Shared Assessments Program. 2017.]
## TABLE 2: THIRD PARTY RISK MANAGEMENT – RISK RATING GUIDELINE

**TPRM Team Activity High Level Checklist**

<table>
<thead>
<tr>
<th>TASK</th>
<th>RESPONSIBLE PARTY</th>
<th>COMPLETE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Develop Outsourcer-Appropriate Risk Rating (Scoring) Criteria and Classification</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Involve all stakeholders</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set rating criteria (based on pre-established key control indicators required to manage each identified risk category)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Formalize the rating process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide awareness training</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide a contract template that allows for relevant requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Inventory All Third Parties</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compile matrix of all potential third parties</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish roles and responsibilities for administration of third parties</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review each third party for:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Financial viability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Reputational risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Appropriate references</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Past/existing judgments or sanctions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Regulatory and compliance requirements specific to the relationship and product/service provided</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Determine Assessment Activity Based on Risk Rating</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rate each third party on the scale against the pre-established criteria</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For each inventoried third party, establish relationship between rating and assessment activity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define ongoing monitoring/assessment for each rating/third party provider type</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Based on the outsourcing relationship, additional activities may need be to be undertaken.

## TABLE 3: COMMONLY EMPLOYED RISK RATING COMPONENTS

<table>
<thead>
<tr>
<th>KEY RATING AREAS</th>
<th>KEY ELEMENTS</th>
</tr>
</thead>
</table>
| Key Impact Risk Areas | • Operational  
                         • Criticality of Processes  
                         • Concentration  
                         • Compliance  
                         • Reputational  
                         • Financial/Credit  
                         • Strategic (logical, as well as physical security)  
                         • Resiliency/Business Continuity  
                         • Transaction  
                         • Recovery Time Objectives (provider availability)  
                         • Vulnerability to Risk |
| Key Risk Rating Parameters | • Classification of data provided to or accessed by the third party  
                                • Geo-location of third party and/or data in question, and fourth parties  
                                • Technology provider or use of technology to provide services  
                                • Network Connectivity.  
                                • Specific regulatory compliance posture that affects Contracting organization  
                                • Provider Business Continuity Program (BCP) / Disaster Recovery (DR) program conformance with outsourcer  
                                • Level of financial commitment for the outsourcing organization  
                                • Criticality or materiality to the outsourcing organization’s operation, including consideration of sole provider third parties |

---

**SHARED ASSESSMENTS**

The Shared Assessments Program has been setting the standard in third party risk assessments since 2005. Shared Assessments, the trusted leader in third party risk assurance, is a member-driven, industry-standard body with tools and best practices, that injects speed, consistency, efficiency and cost savings into the control assessment process. Shared Assessments Program members work together to build and disseminate best practices, building resources that give all third party risk management stakeholders a faster, more rigorous, more efficient and less costly means of conducting security, privacy and business resiliency control assessments.

P: (505) 466-6434  
F: (505) 466-3111  
E: info@santa-fe-group.com

© 2017 The Santa Fe Group,  
Shared Assessments Program.  
All Rights Reserved.
THANK YOU TO OUR CONTRIBUTORS
This is one in a series of papers on best practices in third party risk management. We’d like to thank the Shared Assessments Best Practices Group volunteer subcommittee members who conducted this effort:
- Sridhar Gundrothu, Lead Solutions Architect Third Party Supplier Security, Genpact USA
- Emily Irving, AVP, Vendor Risk & Oversight Manager, Wellington Management Company LLP; Best Practices Committee Vice-Chair
- Brad Keller, Senior Director Third Party Strategy Risk & Compliance, Prevalent, Inc.
- Shawn Malone, Founder & CEO, Security Diligence, LLC; Best Practices Committee Chair
- Melodie Vincett, Third Party Risk Assessor, Early Warning Services, LLC

We would also like to acknowledge The Santa Fe Group, Shared Assessments Program subject matter experts and other staff who supported this effort:
- Bob Jones, Senior Advisor
- Katherine Kneeland, Senior Project Manager
- Charlie Miller, Senior Vice President
- Marya C. Roddis, Vice President, Communications

Consider self-regulation by adopting higher security standards in products and services prior to going to market, even if cost is prohibitive. It’s no longer just the role of government or law enforcement to stop cyber criminals—since networked technology can be weaponized and used against individuals and third parties. It’s in a business’s best interest to be a good corporate citizen.

Stroz Friedberg
2017 Cybersecurity Predictions

ABOUT THE SHARED ASSESSMENTS PROGRAM
The Shared Assessments Program is the trusted leader in third party risk management, with resources to effectively manage the critical components of the third party risk management lifecycle. Program resources are: creating efficiencies and lowering costs for all assessment participants; kept current with regulations, industry standards and guidelines and the current threat environment; and adopted globally across a broad range of industries both by service providers and their customers.

Shared Assessments membership and use of the Shared Assessments Program Tools: The Agreed Upon Procedures (AUP); Standardized Information Gathering (SIG) questionnaire and Vendor Risk Management Maturity Model (VRMMM), offers companies and their service providers a standardized, more efficient and less costly means of conducting rigorous assessments of controls for cybersecurity, IT, privacy, data security and business resiliency. The Shared Assessments Program is managed by The Santa Fe Group (www.santa-fe-group.com), a strategic advisory company based in Santa Fe, New Mexico.

Shared Assessments offers opportunities for members to address global risk management challenges through committees, awareness groups, interest groups and special projects.

Our papers, articles and research studies are written and conducted by industry leaders – members of Shared Assessments Program Awareness Groups, The Santa Fe Group’s partners, consultants and advisors – and cover the hottest, member-driven topics in risk management and business innovation.

Join the dialog with peer companies and learn how you can optimize your compliance programs while building a better understanding of what it takes to create a more risk sensitive environment in your organization.

For more information on Shared Assessments, please visit http://www.sharedassessments.org.

Building Best Practices: Risk Rating Third Parties: Optimizing Risk Management Outcomes