Fourth Party Risk Management: Supply Chain Issues and Emerging Best Practices
ABSTRACT
Risk from downstream parties is increasing as outsourcing organizations engage more and more third parties who themselves have their own outside provider relationships. The proliferation of fourth party relationships provides the undesired opportunity for the existence of major risk management gaps.

Evaluation of third parties and the related regulatory and other risk management issues that resonate through the supply chain is an expansion of the scope of how we typically think about risk management programs. As a third party provider takes on risks, which may or may not be visible and/or controllable by the original outsourcer, the differences between third, fourth, fifth or even tenth party risk and security controls become increasingly nuanced, less transparent and ever more complex.1

As the original outsourcer assumes the risk for its own resiliency and reputation, this trickle-down effect demands close attention for effective solution building. Across most industries, fourth parties are not contractually obligated to share information with clients of their clients. This poses significant problems for an outsourcing organization that naturally needs to know what supply chain parties have access to its crown jewels, such as intellectual property (IP) and personally protected identifiable information (PII), and what risk postures and protections are in place at the down-chain party levels.

This paper focuses on considerations for building an organization’s Fourth Party Risk Management program:
• Examining fourth party risk management evaluation in light of regulatory and non-regulatory issues throughout the supply chain; and
• Discussing emerging best practices and guidelines surrounding fourth party risk management.

Organizations seeking to adopt best practice strategies and methodologies for a start-up program, or, to bolster an existing risk management program, will find it useful to examine what solutions have been successful for peer organizations. For risk managers who are outsourcing to third (and potentially fourth) parties, best practices incorporate:
• Examining and cataloging what processes are outsourced.
• Clarifying the nature and value of specific relationships.
• Educating third parties on required roles and responsibilities for down-chain contractors.
• Obligating third parties contractually, in an actionable way, to an acceptable level of subcontractor monitoring that is commensurate to the risk presented by each fourth party.
• Determining what reporting and accessibility is relevant to meet the outsourcing organization’s unique risk expectations, and what requirements might be necessary to impose at the fourth party level.

Advantages of such a robust, evidenced-based fourth party risk management effort can include: (1) reduction in assessment and remediation efforts and total risk exposure; (2) improved provider selection processes; and (3) more meaningful due diligence, risk monitoring information and review. These benefits can allow an organization to identify concerns with a third or potential fourth party of which the risk team may be otherwise unaware.


**ISSUE LANDSCAPE**

Combined with the increased use of outsourced services, new rules and an evolving threat environment are driving the need for enterprise-wide third party risk management processes. The processes that ensure that the risk controls of third parties, as well as the subcontractors of those third parties, should mirror the outsourcer’s risk appetite.

In this relatively immature fourth party management space, clear guidelines and uniform processes have not been established. This has resulted in non-standardized, cumbersome and disjointed documentation processes that generally provide an incomplete view into third and fourth party risk management issues.

The resultant potential exposure to risk applies to all supply chain components, including professional and support services, manufactured goods and other elements of the logical (information) and physical (goods) supply chains. This means that fourth party relationships have the capacity to create unacceptable risk around business resiliency and other negative effects throughout the supply chain.

By 2019, the need for transparency into operational and security activities within a vendor’s value network (including subcontractors) will drive demand for vendor security, as well as risk management solutions and services, by 30%.

**The Current Risk Management Climate**

The risk management climate is increasingly focused on outsourcing vulnerabilities, and mandates that organizations know more about their third parties and how those relationships can affect the outsourcer’s business.

There is expanded regulatory scrutiny of asset and information security and management that involve any outsourcing vulnerabilities, and mandates that organizations know more about their third parties and how those relationships can affect the outsourcer’s business.

Due to requirements in the risk management arena for monitoring and testing of an outsourcer’s third party risk management programs, fourth parties that can impact the risk position of third party providers have come under examination and now require direct board oversight.

As a result, a wide range of constituencies have begun to recognize the risks associated with third and fourth party providers and the need to increase program maturity to levels that ensure inclusion of consistently applied criteria for provider risk classification or rating. This is reflected in the 2016 Vendor Risk Management Benchmark study findings where use of risk classification or rating maturity levels increased significantly between 2015 and 2016.

More outsourcing organizations (nearly 90%, up from 75% in 2014) are also reporting they identify and/or maintain an inventory of their fourth parties. This demonstrates that fourth party oversight is gaining ground, despite having been included in the top three areas of focus by regulatory body review oversight only 8% of the time during reviews.

However, the level of rigor in programs varies as to how organizations assess and/or monitor their fourth parties:

- Twice as many outsourcing organizations (75%) now rely on controls of their third party to monitor fourth parties than two years ago; and 73% report they use contractual terms to achieve this process.
- There was a 28% drop (from 84% to 56%) in outsourcing relationships that to have and enforce contractual terms with their fourth parties as a means of fourth party assessment and/or control.
- Just 8% of outsourcing organizations report they now rely on their relationship manager program to assess/monitor their fourth parties; down from 56% in 2014.
- 78% of outsourcing organizations report they identify fourth parties during the contracting phase (up from 60%).

These responses demonstrate both that the landscape is adapting to fourth party concerns, and that issues still exist around reporting and accessibility of information at the fourth party level. For example, in the 2016 Ernst and Young study, the use of contract templates that include service level agreements (SLAs) that push third parties to ensure their providers meet defined risk control requirements is increasing. Such individual and group provider relationship controls are critical, as for providers that handle confidential data and may be consumer facing. Three-quarters of organizations in the financial services sector now rely on controls of their third party to monitor their fourth parties, representing an emerging best practice.

**Emerging Guidelines**

While no single industry has established a standardized resource for fourth party risk, the insurance industry’s focus on aggregation risk provides a window into this area, especially with reference to security issues.

National Institute of Standards and Technology (NIST) guidelines for risk-based strategies provide a basis for fourth party requirements:

- Link risk management activities to the outsourcer’s mission.
- Establish responsibility for controls throughout systems.
- Encourage use of automation to increase consistency, effectiveness and timeliness of control examination and mitigation.
Fourth party outsourcing risks to consider.

OUTSOURCING RISKS
• Financial
• Strategic
• Reputation
• Geolocation
• Credit
• Quality

POSSIBLE IMPLICATIONS
• Difficulties or failures
• Misalignment with objectives
• Brand/organizational impacts
• Consent orders, fines and penalties
• Sanctions due to country
• Inability to make payments
• Inability to deliver in line with SOW specs

SERVICE-LEVEL RISKS
• Cyber
• Compliance
• Legal
• Intellectual Property
• Privacy
• Contractual
• Operational
• Resiliency

CAN RESULT IN
• Impacts to confidentiality, integrity or availability of information/services
• Non-alignment with standards/frameworks
• Failure to meet contract obligations
• Failures that impact operations
• Inability to provide services

A FOURTH PARTY is your vendor’s third party or subcontractor and is vulnerable to the same risk as your third parties.

Other rules driving best practices include those from the US Department of Treasury’s Office of the Comptroller of the Currency (OCC), which mandates that “effective third-party processes” are required, including “significant investment in resources to implement the third-party relationship and manage the risk.”12 The requirements of many other financial, privacy and security standards and regulations have implications for fourth party use that can affect companies globally throughout their supply chains. This includes the New York State Department of Financial Services 23 NYCRR 500, FFIEC Cybersecurity Assessment Tool (CAT), International Standards Organization (ISO) 27001/27002, Payment Card Industry (PCI) DSS v.3.2, as well as anticipated EU General Data Protection Regulation (GDPR) rules and Cloud Security Alliance (CSA) Controls.

BEST PRACTICES METHODOLOGY GUIDELINES
Robust risk management practices in this third/fourth party arena now include: controls dedicated to appropriate and ongoing training; detecting possible malicious activity; and mitigating attacks and fixing core problems within programs and systems.

Access to information comes primarily from reviewing the evaluation/monitoring process of each third party’s providers, rather than direct fourth party evaluation.

The process of outsourcing should automatically trigger a chain of screening, assessment, evaluation, documentation gathering and ongoing monitoring. Such efforts mandate the involvement of all stakeholders (internal and external) within the supply chain to be effective in establishing:
• a complete understanding of roles and responsibilities;
• reporting accountability;
• the outsourcer’s third party environment; and
• a well-documented set of processes and procedures.

Without such controls, there may be confusion about what each relationship level requires to minimize any issues that can arise around reporting and accessibility to information at the fourth party level.

A process of re-education, similar to that undertaken when the Payment Card Industry (PCI) standards were developed and implemented, is required to ensure that third parties are accountable for ensuring that their down-chain parties meet the outsourcer’s risk needs.

Best practices that address pertinent regulations and meet the needs of industries across all verticals include:
• Documented planning and due diligence that involves all stakeholders: This includes risk rating, contract negotiation, ongoing monitoring (including
continuous monitoring), planning for termination, clearly established and documented third party relationship managers, oversight and accountability and reporting and independent reviews. While most organizations will evaluate controls at the fourth party level, some will continue to evaluate to the "n"th level based on the outsourcer’s risk appetite.

- **Use of fourth party specialists:** If a provider is critical, it is best practice to get a fourth party specialist, (either an internal employee or an external firm) to coordinate and integrate the resources of all components of the supply chain and review periodic reports based on established fourth party attributes.

- **Implement Smart Database/Warehouse tools:** Creation and maintenance of an advanced, enterprise-wide information base that allows for evaluation of fourth party providers, (initial and ongoing) regarding the use of outsourced third and fourth parties to drive decision making. It should include such information collection as lists of third party locations, as well as fourth party stakeholders. This involves an appropriate platform for managing a fully developed, up-to-date inventory of third and fourth party providers (and the services they provide).

- **Understand supply chain dependencies:** Examination of the dependency and any concentration risk presented by the outsourcer’s third party providers. This examination must also include an understanding of the impact fourth parties may have on business resiliency and the ability of all parties to meet outsourcer and other upstream supplier contractual obligations. Third party providers should have formal contingency plans in the event that fourth party provider products/services become unavailable. This information allows an outsourcer to determine a specific set of fourth parties for certain uses.

- **Periodic third party reporting:** Account management meetings should include review of key contract obligations, such as where data is stored and processed, whether or not fourth parties are involved and any changes to data processing or other critical functions. Meetings should be held at pre-established cycles (frequency tied to the provider’s risk rating). Third party should have documented evidence, such as industry certifications and independent assessments, of how it gained fourth party risk posture assurances. That documentation should be accessible to the outsourcer. Contract language can be added requiring continuous monitoring of fourth parties and adverse event disclosure to outsourcer, such as data breaches, litigation, or complaints that could affect the outsourcer’s risk position.

- **Training and communication:** Education of outsourcer third and fourth party relationship staff and/or independent reviewers on all SLAs, regulatory requirements and standards to which the outsourcer is subject. There is commonly one team that manages engagements and one that manages contracts, which may mean security team silos may not understand SLA implications without specific training.

- **Stay aware of shifts in regulatory climate:** All organizations should have mechanisms to monitor changes to regulations and standards that apply to their own organizations, as well as to their providers, and set up processes and contract allowances that facilitate an agile response. This may be done internally, or outsourced to a third party that merges traditional assessments with tracking and analyzing industry-specific requirements.

The following metrics address these best practices concerns. These metrics apply to both regulated and unregulated industries, allowing for examination of supervisory strategies, material changes to relationships and/or management processes, key party inventories, and the quantity of risk and the quality of risk management.

The metrics to be applied should be identified during contract negotiation include:

- **An auditable (documented) risk rating scale.**
- **An inventory matrix** showing the general business vetting indicators that will be assessed. This may include, but should not be limited to: financial viability, reputation, appropriate references, existing or past judgments or sanctions, regulatory and compliance requirements specific to the relationship (such as HIPAA, PCI, industry required certifications, etc.).
- **Specific use, access and permitted data volume allowances.** Criteria should be set and monitored for appropriateness, with any changes being conveyed to all stakeholders, as needed.
- **Indicators that can realistically be gathered**, including information that allows for determination of whether fourth parties are in use that place, or may place, the outsourcer at risk.
- **Include “trigger events”** with defined escalation incumbent upon the third party to report to the outsourcer. Examples may include: changes to infrastructure/network design (year/assessment cycle, etc.); and operating system, backup, or other information or security system alterations.
- **Analysis and dashboard capabilities** presented in a meaningful fashion; i.e., that allow for analysis and application of metrics against pre-established criteria.
- **Regulatory awareness monitoring** to allow for response to changes in a given geopolitical or industry area or the related impacts of concentration risk by industry or service (e.g., data centers, cloud).
- **Indicators of third party organizational resiliency,** such as mergers and acquisitions and other salient information, that might indicate potential or imminent shifts in the third and fourth party’s stability.

While building or adapting a third/fourth party risk program, stakeholders should remain cognizant that there is a point of diminishing returns for seeking information.
within the levels of the supply chain. Data collection that drives down several levels would be based on how far down the supply chain risk is known to exist. This examination can include continuous monitoring efforts, which can increase the amount of data noise in the monitoring system.

Defined programs can control this data noise by developing systems that provide sufficient information for decision making and escalation processes. Determine where fourth party risks exist that are critical, so as not to inundate the resources allocated to monitoring. Specific risk rating areas and categories that may be considered for inclusion in an organization’s reporting requirements are included in the takeaway guideline table at the end of this document.

**BENEFITS**

Development of rigorous third party risk management program must include due diligence surrounding fourth parties. This due diligence should include, continuous monitoring and high-value metrics that are presented on a well-planned dashboard, to allow risk managers greater insight into potential concerns with a third or fourth party.

Traditional approaches require a significant amount of resources and time for assessment of a single third party. A study of 470 risk managers demonstrated wide agreement that a robust, common platform enhances risk management and supports improved reporting to senior management and the company board. It also provides an effective platform method for extending enterprise-wide risk management processes and priorities, as well as improving productivity and accuracy of the risk management team.

An organization can employ their own return on investment (ROI), results-based-accountability model to set efficiency targets based on:
1. The cost related to the number and depth of assessments required for its third parties.
2. The cost related to potential risks (e.g., a breach, loss of data, loss of continuity, etc., and the related income or market share losses).
3. The operational savings that can be achieved through the efficiencies of a centralized, best practice based third/fourth party risk management program.

Return on investment for a robust fourth party risk management effort can include:
- Reduction of effort by leveraging elements of an existing, mature third party risk management program or incorporating strategies and methodologies that are known to be successful and adopted from outside sources, resulting in reduced total cost of risk.
- More digestible due diligence and monitoring information can be provided to review teams and committees, providing context-oriented details that are simplified and translated into actionable content.
- Advantages with respect to prioritization and selection of third party providers.
- A more realistic understanding of the potential financial or other impacts of third and fourth party relationships, that can provide improved issue identification and reduction in time to remediate through a more transparent process that highlights potential and actual down chain risks.

**CONCLUSION**

Ensuring security and compliance for all supply chain components has become mission-critical. To protect their reputation and overall sustainability in the market, outsourcers have to adopt more holistic strategies for third party provider management.

The outsourcing organization can expect to significantly improve the impact of its risk management efforts by:
- Including all stakeholders in risk planning, management processes, appropriate training and communications with third parties; and
- Defining expectations and reporting requirements around third and fourth party risk management.

This approach ensures that the same standards apply throughout the supply chain as the outsourcer defines the overarching set of control requirements that it deems appropriate to maintain its own risk posture. Not only will such efforts provide measurable returns on investment in operational efficiency, organizations that employ emerging best practices will become more effective at identifying and mitigating down-chain threats.

---

1. Parties within this paper are defined as: Outsourcer – the entity delegating a function to a subcontractor; Third Party – the subcontractor 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.
10. Shifting toward maturity: Key findings from EY’s 2016 financial services third-party risk management survey. EY. June 2016.
16. In the outsourcing context, concentration risk can be defined as the probability of loss arising from a lack of diversification. BITS Guide to Concentration Risk in Outsourcing Relationships. BITS, 2010.
17. The ROI of RMs. Riskknect. 2015.
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:
• Marlin Arnholz, Senior Vice President, IT Risk Manager, Northern Trust Corporation
• Erik Bataller, Vendor Application Security Testing Manager, Veracode
• Elisa Cady, AVP, Fourth Party Risk Compliance Specialist, U.S. Bancorp
• Barbara Cochran, Third Party Risk Assessment Officer, U.S. Bancorp
• Jeff Coughlin, Supplier Risk Manager, Principal Financial Group
• Leo Cuellar, Manager, iovation
• Gaurav Deep Singh Johar, Assistant Vice President, Enterprise Risk and Compliance, Genpact USA
• Patricia Enfanto, Senior Manager Supplier Security Management, Philips
• Cory Faust, Risk Consultant, TSC Advantage
• Sridhar Gundrothu, Lead Solutions Architect Third Party Supplier Security, Genpact USA
• Christina Howlett-Perez, Manager, Procurement, Wellington Management Company LLP
• Emily A. Irving, AVP, Vendor Risk & Oversight Manager, Wellington Management Company LLP
• Shawn Malone, Vice President, Business Compliance, Radian Group, Inc.
• Tony Manley, Director Vendor Management, MERSCORP Holdings Inc.
• Anthony Mastrolembo, Vendor Risk Management Program Manager, Freddie Mac
• Kelly Milliken, Threat Analyst, TSC Advantage
• Juliet Okafor, Vice President of Global Business Development, Fortress Information Security
• Jake Olcott, Vice President Business Development, BitSight Technologies
• Sesha Vellala, Senior Principal Consultant, Genpact India
• Joel Wuesthoff, Senior Director, Protiviti, Inc.

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

ABOUT THE SHARED ASSESSMENTS PROGRAM
The Shared Assessments Program has been setting the standard in third party risk management since 2005. Member-driven development of program resources helps organizations to effectively manage the critical components of the third party risk management lifecycle by creating efficiencies and lowering costs for conducting rigorous assessments of controls for cybersecurity, IT, privacy, data security and business resiliency. Program Tools are kept current with regulations, industry standards and guidelines and the current threat environment; and are adopted globally across a broad range of industries by both 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 for third party risk management programs. 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.

Join the dialog with peer companies and learn how you can optimize your compliance program. For more information on Shared Assessments, please visit http://www.sharedassessments.org.

Many companies perform due diligence and monitoring on their direct vendors, but those legacy minimums are no longer sufficient: reputational and compliance liabilities extend further down the supply chain now than ever before. Companies must safeguard themselves against vendor’s vulnerabilities – especially with regard to information security – across their entire supply chains, extending from their direct vendors to secondary and tertiary suppliers, service providers, and shippers. The situation demands that executives carry out a progressively difficult mission: to reduce risk while sustaining rapid decision making and to price competitively as they meet global demand.

PwC
**APPENDIX I: FOURTH PARTY RISK MANAGEMENT GUIDELINE**

Table 1: Process areas for third party provide assessment that impact review of fourth party risk posture

<table>
<thead>
<tr>
<th>REVIEW AREA</th>
<th>INDICATOR</th>
<th>TECHNIQUES</th>
</tr>
</thead>
</table>
| Third Party Selection | • Are all parties that touch sensitive data identified and a risk assessment performed prior to gaining access? This includes call and data centers, as well as other outsourced service providers.  
• Are all parties that are consumer facing (direct contact, mail/email or systems) identified and a risk assessment performed prior to gaining access to the outsourcer’s consumer customers?  
• Is a system in place that is aligned with a documented risk rating and assessment process for all down chain parties?  
• Is an action plan in place for remediation?  
• Do contracts define roles and responsibilities, including monitoring of specific risk factors that are mission-critical and compliant with regulations?  
• Are all of the outsourcer’s mission critical third parties with fourth parties identified and risk assessed during the third party selection phase?  
• Are all of the outsourcers able to identify if data resides in the cloud (private/public) and risk assessed during the third party selection and ongoing monitoring phases? | • Fourth party SLAs or contract template(s) that include requirement of a risk management program comparable to the outsourcer’s third party risk area requirements.  
• Automated collection of publicly accessible data (news, data collection and reporting agencies, management dashboard tool providers, etc.) that divulge fourth party relationships, even if the third party provider has not divulged those to the outsourcer.  
• Security Information and Event Management (SIEM) documentation demonstrating follow through of reported material event(s). |
| Monitoring           | • Is there documentation of fourth parties that a third party provider has changed or newly contracted with since the last assessment report?  
• What is the third party’s continuous monitoring process, and what is their SLA commitment to do so? | • Defined escalation triggers.  
• Additional monitoring techniques for fourth parties that support specific services (e.g., consumer facing fourth party customer complaint policies; mission critical third party participation in fourth party disaster recovery exercises; data processor adverse event policies). |

**APPENDIX II: COMMONLY EMPLOYED RISK RATING AREAS AND CATEGORIES**

<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 provider.  
• Geo-location of third or fourth parties (and/or data in question).  
• Technology provider or use of technology to provide services.  
• Specific regulatory compliance posture that affects Contracting organization.  
• BCP/DR program conformance with contracting organization.  
• Level of financial commitment for the contracting organization.  
• Criticality or materiality to the contracting organization’s operation, including concentration risk (limited or sole providers).  
• Degree of fourth party reliance.  
• Access of consumers to services. |

The Shared Assessments Program has been setting the standard in third party risk assessments since 2005. Shared Assessments, the trusted source 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.