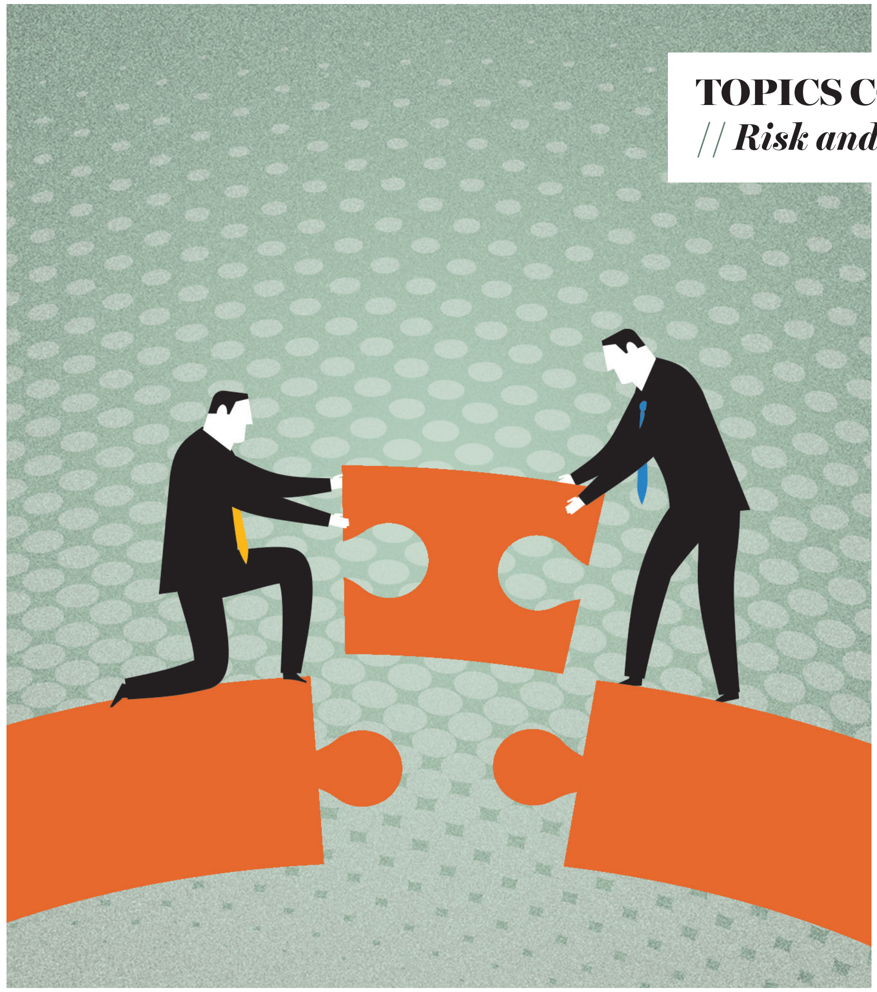


TOPICS COVERED
// *Risk and Strategy*

EFFECTIVE INTEGRATION

A Practical Guide to Third Party Risk

Written by James E. Williams and Jill M. Williamson

There is more to a successful Third Party Risk program than risk rankings and questionnaires. A successful program relies on buy-in at all levels and integration with existing processes and controls. If your third party risk program is administered by the legal and/or compliance team working in a vacuum, you may be doing more harm than good. Third party risks run across many functions and new risks are arising with more frequency.

Finance / Accounting

In many ways, the accounting and finance function is the most important function for mitigating third party risk. The finance team plays two crucial roles in third party risk mitigation:

1) Implementation of compliance controls
Many risk controls require continued monitoring by those that pay the bills. Some examples include invoicing requirements to ensure compliance with contract requirements such as restrictions on using sub-contractors and interface with government officials, and invoice detail and supporting documentation requirements.

2) Identification of red flags
Those that pay the bills are also in the best position to identify certain red flags. Some examples of such red flags include third party, third country, or third country currency payment instructions, repeated failures to comply with contract restrictions, generic or vague descriptions for services rendered, or questionable service fees, expediting fees, or gifts and entertainment.

It should be noted that third party compliance risk controls may differ significantly from traditional SOX or accounting controls. Traditional SOX/accounting controls are primarily based on a binary financial threshold, i.e. payments over $5,000 require two signatures. Compliance risk controls that are responsive to business needs have more components; e.g. payments to high risk third parties, in certain regions, require heightened scrutiny or higher levels of approval. Implementation of these controls will require revision of the accounting practices guidelines, training of relevant individuals, and adjustments to software systems used for these processes.

Key discussion points for Finance/Accounting:

- What are the existing controls, how are they implemented and what software is used?
- How to recognize red flags, what to do when they are spotted.
- How many and what types of third parties are there, or how can that be determined?

Business Stakeholders

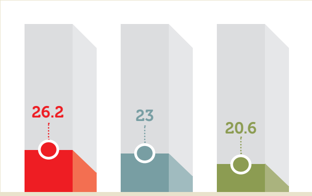
A third party risk program will be most successful if it is designed to meet business needs. "Business partners" include the sales and marketing functions, customer facing departments, as well as operational / fulfillment functions. Meaningful consultation with key business stakeholders actually acts as a complement to business success. When consulting with business stakeholders, ascertain what their key concerns and perceptions are regarding a third party risk program. Common concerns include slowing of the sales / contracting processes, termination of successful long-standing relationships due to red flags, and offending long-term partners with questions about ethics. Not all of these issues can be avoided; after all, the point of a third party compliance mitigation program is to gather relevant information to allow the company to make informed decisions about risk. In some cases, that decision might be to terminate a relationship, but in other cases, the right decision might be to add controls, monitor the relationship, or even assist the third party to build the appropriate compliance framework. By maintaining an open dialogue, the right balance can be reached.

Business partners also provide specific information helpful for building a program responsive to business needs.

Key discussion points for business stakeholders:

- What risks do you worry about? What reputational issues do they think would have a negative impact on sales or shareholder value?
- What are they doing to mitigate those risks currently?
- Which third parties are used in the business, what the pipeline is for various third parties, and the rationale behind using third parties for various activities?
- What the due diligence is expected to look like, what might constitute a red flag, and what some options are for dealing with them?
- What further steps are needed when a red flag arises? In many cases, depending on the type of red flag, further inquiry may be required before making a decision.

Facts & Figures



*According to Deloitte's Third Party Governance and Risk Management Survey 2016, **26.2 percent** of organizations have suffered reputational damage, **23 percent** have been non-compliant with regulatory requirements and **20.6 percent** have experienced a breach of sensitive customer data.*

Procurement

The procurement function often provides the basic framework within which the third party risk mitigation program will sit. Understanding how the existing procurement process works, which third parties go through it, which risks are already being addressed, and how, will provide the baseline to determine the most efficient implementation for the third party risk program. An advanced procurement system, that already has mechanisms for collecting information and ranking third parties with respect to financial or supply chain risk, should be easily adaptable to incorporate additional compliance risks. Less sophisticated systems may not provide the same baseline, but on the upside, they may provide a relatively blank slate for the company to address risk.

Key discussion points for procurement:

- Which third parties, if any, go through procurement?
- What is the existing onboarding system, what software is used, and what risks are already addressed?
- Can additional functionality be built into the onboarding system to better monitor compliance risks?
- How can the current system be best modified to incorporate compliance risk?
- Which reports can the system generate to monitor compliance risk?
- How many and what types of third parties are there, or how can that be determined?

Numbers, Numbers, Numbers

There are a few key metrics that can assist in planning the program implementation, risk assessment, planning a monitoring program and reporting. Careful husbandry of metrics is also useful in setting expectations with key stakeholders. The metrics you choose should be tracked and analyzed for trends so your program is responsive to changes. Potential measurements include:

- How many third parties exist in each risk category?
- How many third parties have risk controls implemented?
- How many third parties have had red flags, either during on-boarding or afterward?
- If you are screening third parties through restricted party lists, such as the OFAC Specially Designated Nationals list, the percentage of records that match, and how many are 'good matches' v. 'false positives.'
- Number of compliance incidents, such as hotline reports, internal or external investigations, violations of law or policy, and incidents arising out of third party activities.
- The percent of revenue that is generated through third party agents and/or percent of activities that are performed by third parties.

A successful third party risk program addresses the risks impacting different functions, takes into account the priorities and needs of each function, integrates with their key processes and systems, and is flexible enough to include new risks that arise over time. Effective collaboration with each constituency and the use of detailed metrics will enable your company to effectively navigate this increasingly complex area.

Author Biography

***James E. Williams** served as Vice President, General Counsel, and Corporate Secretary at Liquidity Services from November 2005 - April 2016. James contributed to the Company's market leadership by building the legal, compliance and risk management team and counselling the Board and executive team on all governance, legal and risk management matters.*

***Jill M. Williamson** is of Counsel at Rimon Law where she advises clients on a wide variety of compliance matters. She has served in house as the Chief Compliance Officer at Liquidity Services, Inc., where she built their compliance program from the ground up and as Deputy Chief Compliance Officer at Cigna.*