Third-party Risk Management

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

This is the first installment of a new column, The Practical Aspect. This column is designed to achieve
the following goals.

- Identify practical aspects of current professional challenges that may not have been adequately documented yet.
- Bridge these aspects with existing concepts, theories and paradigms in an effort to clarify or support existing practice.
- Generate further inquiry/debate on developing the issues further for the benefit of the practicing IT professional.

The business model of the early 20th century depicted a large, integrated company that owned, managed and directly controlled its resources. Whereas some procurement was not beyond scope, much of the value creation was meant to occur within the company. In the later decades of the 20th century, outsourcing emerged as a strategic, tactical and operational maneuver. The reasons to outsource varied and became more sophisticated over time, including the need to:

- Reduce and control costs
- Improve host company focus
- Gain access to world-class capabilities; augment internal resources for other purposes
- Share risk and rewards with the vendor[1]

Specifically in the software services area, the relationship complexity increased as the expected business value from the services grew in focus, from efficiency to enhancement to transformation.[2] Depending on the criticality of the relationship in value creation and its attendant risk, the third party, for all practical purposes, became an integral driver of the host company's destiny. Such relationships sometimes are categorized in terms of structure (e.g., collaboration, alliance, partnership, joint venture) and, in other instances, they emphasize the nature of products or services (e.g., facilities management, human resource services, software maintenance, telecommunications, logistics/warehousing/distribution).

Business leaders have recognized outsourcing as essential to remaining competitive. In a survey, 90 percent of responding firms cited outsourcing as crucial to their growth strategies.[3] This momentum continues to gain further strength as the comparative advantage of collaborating in various forms across the globe is clearly visible and remarkably effective. Over time, as the host becomes more dependent on the vendor, the

Vasant Raval, DBA, CISA, ACMA
Is a professor of accountancy at Creighton University (Omaha, Nebraska, USA). The coauthor of two books on information systems and security, his areas of teaching and research interest include information security and corporate governance. He can be reached at vraval@creighton.edu.

Samir Shah, CISA, CA, CFE, CIA, CISSP
Is an executive director at Ernst & Young LLP. He has many years of experience in the IT risk, audit and governance-related practice areas. He can be reached at samirnshahca@gmail.com.

opportunity for the host's risk to be exposed by the vendor increases as well. When this happens, the emphasis on the third party diminishes greatly, for the hosts see the relationship as far more closely tied to their own destiny than anticipated. It is as if a crucial part of the business's success now resides in the vendor organization, making the vendor more of an "insider." If some risk materializes at the vendor level, depending on the nature of the relationship, cascading effects of the compromise could engulf the host as well. This is considered a form of yet unaddressed or unknown "vulnerability inheritance," triggering heightened risk awareness at the host level.[4] Risk in third-party arrangements of any form have always existed, but the mix, in terms of types and severity of risk, has been changing, leading to a reexamination of the host-vendor relationship primarily from the risk management perspective. Hence, the term "third-party management" is now more clearly emphasized as third-party risk management (TPRM).

> **"The focus of multifaceted outsourcing converges heavily on managing the risk exposures of the relationship."**

The legacy risk of TPRM includes financial and operational risk. Cyberspace and related connectivity add new (or enhanced legacy) risk, such as business continuity, data security, and regulatory and compliance risk. Thus, the focus of multifaceted outsourcing converges heavily on managing the risk exposures of the relationship. The goals of TPRM may include, for example, favorably impacting data breach consequences, lowering risk of operational failures in a supply chain, continuously monitoring vendor financial stability, and assessing the risk of governance and regulatory disclosure.

TPRM Methodology

Broadly, any risk management program is three-dimensional. It incorporates people (organization), process (operations) and technology (information systems). Each is important to the TPRM goals and plays a significant role in achieving the desired outcome.[5] The TPRM methodology discussed here incorporates all three dimensions.

To address risk exposures in TPRM environments, host companies consider the vendor as the target of evaluation at the time of onboarding and on an ongoing basis as well. For this, the host company should:

1. Set up contract provisions (typically, in the service level agreement [SLA]) to address risk-related commitments
2. Combine the vendor risk profile with the risk profile of the engagement
3. Prepare for dynamic monitoring and risk assessment based on internal/external events
4. Implement and use both traditional and innovative monitoring approaches for continuous monitoring of the identified risk factors
5. Leverage technology solutions to integrate procurement, performance and risk management on a unified platform[6]

The SLA in the first step would include the host's right to audit and responsibility for related costs, enrollment of the vendor on the agreed-upon TPRM utility platform, incentives for proactive risk management by the vendor, and requirements for insurance coverage of risk areas by the vendor. A complete risk profile of a vendor for an organization results from the aggregation of inherent risk of the engagement for which the vendor is hired and

Enjoying this article?

- Read ***Vendor Management Using COBIT® 5.*** *www.isaca.org/vendor-management*
- **Learn more about, discuss and collaborate on risk management in the Knowledge Center.** *www.isaca.org/risk-management*

inherent risk from the vendor profile. It helps in focusing on the right subset of vendors for effective and efficient TPRM.

An ongoing assessment of risk as events unfold is important for dynamic risk management. This would likely be accomplished by continuous monitoring activities. As the final step suggests, the entire effort can be far too complex to leave it to fragmented solutions; an integrated, IT-enabled platform would be the most effective way to generate a successful TPRM program. **Figure 1** presents an overview of a TPRM methodology.

> **"Today's interorganizational risk management challenges are more complex than what an extended and elaborate SLA document can effectively manage."**

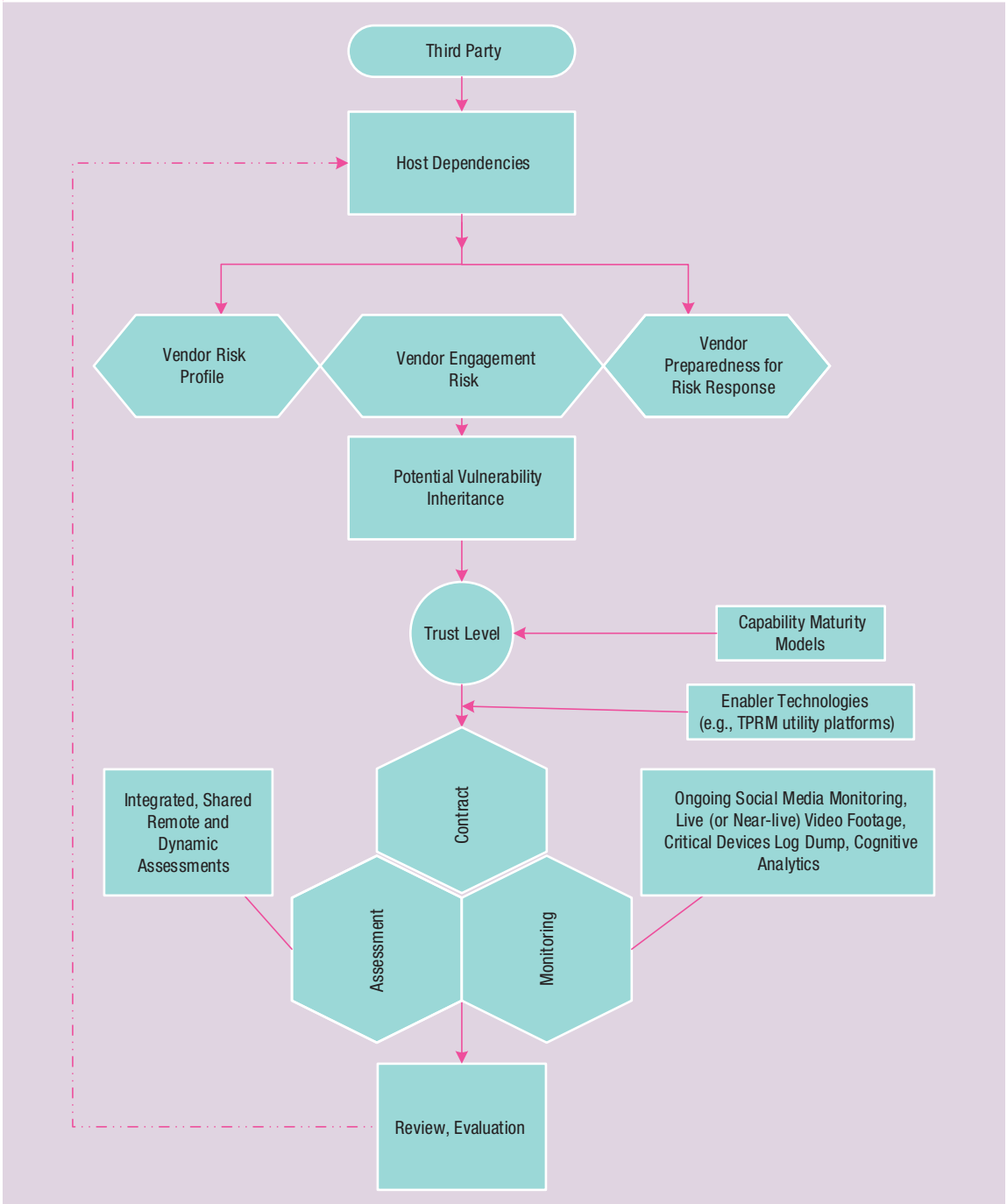
TPRM and Information Technology

The rise of TPRM as a challenge probably took place due to the now well-known hack of Target. While the IT-based Target compromise elevated TPRM to new heights in the information security domain, many additional areas (e.g., supply chain and logistics) are also managed through TPRM.[7] And this, therefore, leads to the need for trust between the host organization and its stakeholders, including vendors. Presumably, the greater the criticality of the service, the higher the need for trust, much as in the authentication of people or devices. Without trust, not much can be considered in equilibrium in the relationship. When Amazon cannot find enough digital streaming capacity between 11:00 p.m. and 2:00 a.m. to serve Netflix customers, would Netflix be able to trust Amazon? When such questions are resolved dynamically, the host-vendor trust solidifies and continues to support an interorganizational, synergistic supply chain.

Agile and effective trust relationships rely on governance practices, but most organizations working with third parties "do not have a coherent plan for the ongoing management of the relationship and the services that are provided. It is often assumed that the contract and the various service agreements…will be self-managing and that investing in governance processes over the contract's lifetime is unnecessary."[8] Given the increasing scope and complexity of the TPRM, as the final step in the TPRM methodology suggests, an integrated IT-enabled platform would serve the TPRM goals best.

Why would a host need an integrated procurement, performance and risk management platform? The reason is that new issues and challenges often do not quite fit the old templates. A mishap at the third-party provider may spell new risk to the seeker of services. To address dynamically the changing risk scenario, an integrated risk management platform is necessary. While standards help guide the implementation of such platforms, Statement on Standards for Attestation Engagements (SSAE) 16/International Standard on Assurance Engagements (ISAE) 3402 (the revised standards for the earlier SAS 70) have known challenges with the coverage of a large population of third parties and efficiency from time and cost perspectives. No matter how robust these assurance standards are, interorganizational dependencies are unique, and uniquely granular, to a point where the solution requires customized due diligence. A contractual shared solution across all vendors may not be enough, for "nothing in business operations remains in a steady state…."[9] A *force majeure* clause in the SLA does not save either party from disasters.

Figure 1—Overview of a TPRM Methodology



Source: V. Raval and S. Shah. Reprinted with permission.

Some Answers

In key relationships where the continued viability of the relationship is predicated on the host organization's superior vigilance and action, exit strategies do not work. Most third parties have an impact on a host organization's destiny; they are not adversaries. Today's interorganizational risk management challenges are more complex than what an extended and elaborate SLA document can effectively manage. Moreover, trust is sourced not just in technology, but also in various related disciplines, and these can be effectively garnered only through multidisciplinary teams accountable for the relationship. Additionally, a holistic approach is probably more effective, where organizations look at the policies, risk management profile and related history, business continuity plans and recent recovery exercises, and going-concern capability both financially and operationally. This type of comprehensive risk monitoring of a provider requires continuous scanning and monitoring by the tasked team on a rather well-scoped dashboard.

The SLAs, though not a complete solution to a holistic TPRM program, have been used as the primary hook in the establishment of the vendor's commitment to manage risk. Expanded SLAs include clauses such as the host's right to audit and may specify the audit scope, the audit process, frequency of auditing and even triggers that may require an unscheduled audit. Such contractual commitments are translated into the planned risk monitoring activities that provide for continuous assessment and review of the TPRM.

Given the complex cyber-based relationships with third parties, the new direction used is dynamic risk profiling to track the relevant engagement risk. Hosts seek financial (and nonfinancial) data about the provider entity from within and from external parties (e.g., Thomson Reuters). Monitoring of the provider may involve machine learning and predictive analytics[10] that "soak up" rapidly emerging data about social media activity, media and public relations coverage, compliance filings, and even random-looking bits and pieces that may help dynamic risk profiling.

"An all-encompassing TPRM becomes an expensive proposition for the parties involved."

The universe of vendors even a modest-size company would deal with is probably quite large and varied in terms of size, location, financial risk, operational risk, emerging technology and innovation risk, and so forth. Some form of ABC analysis[11] of vendors to determine their trust levels could help save on costs while targeting vendor-specific risk through vendor "tiering," where critical vendors could be classified as tier 1 (critical systems), major vendors as tier 2 (moderately critical systems) and other vendors as tier 3 (commodities or low-risk relationships).[12] Nevertheless, an all-encompassing TPRM becomes an expensive proposition for the parties involved. To save on costs and improve process maturity, pooling of interests among peers in an industry (e.g., auto companies, phone companies) has been becoming more popular. For example, TPRM utility platforms such as Markit, where member organizations would require their third parties to enroll on the platform, have been launched. Shared assessment groups (e.g., Santa Fe Group) and shared information gathering tools (SIG) leverage workflow tools, capability maturity model applications

and vendor dashboards not just to lower costs, but also to improve the quality of risk management.

Practice Implications

Reports suggest that 70 percent of companies do not adequately engage in TPRM, yet more than 90 percent indicate they will increase their use of third parties.[13] This anomaly cries out for a practical, cost-effective solution that mitigates risk in alignment with the seeker's risk appetite. The onset of regulatory requirements, such as those from the office of the US Comptroller of the Currency[14] in the financial services industry, is just one indication of TPRM's significance. Enterprise risk management preparedness on the part of those seeking third-party vendors may be lacking at this time. All this adds to the urgency in addressing this rapidly evolving risk management need that simply cannot be avoided in today's business environment.

Author's Note

Opinions expressed in this column are the authors' own and not those of their employers.

Endnotes

1 Handfield, R.; "A Brief History of Outsourcing," North Carolina State University, USA, State, Poole College of Management, Supply Chain Resource Cooperative, 1 June 2006, *https://scm.ncsu.edu/scm-articles/article/a-brief-history-of-outsourcing*

2 Cohen, L.; A. Young; *Multisourcing: Moving Beyond Outsourcing to Achieve Growth and Agility*, Harvard Business School Publishing, USA, 2006

3 Corbett, M. F.; *The Outsourcing Revolution: Why It Makes Sense and How to Do It Right*, Dearborn, USA, 2004, *https://www.economist.com/media/globalexecutive/outsourcing_revolution_e_02.pdf*

4 The Target hack in 2013 provides an example of vulnerability inheritance.

5 Raval, V.; A. Fichadia; *Risks, Controls, and Security: Concepts and Applications*, Wiley, USA, 2007

6 Shah, S.; "Third Party Risk Management—Emerging Trends," ISACA Mumbai (India) Chapter presentation, June 2016

7 Dorr, C.; "Third Party Risk Management," ISACA Cincinnati (Ohio, USA) Chapter presentation, September 2014, *https://www.isaca.org/chapters5/Cincinnati/Events/Documents/Past%20Presentations/2014/Third%20Party%20Risk%20Management.pptx*

8 *Op cit*, Cohen and Young

9 *Op cit*, Cohen and Young

10 Predictive analytics at this time is likely at an incubation stage in TPRM.

11 Business Dictionary, ABC analysis, *www.businessdictionary.com/definition/ABC-analysis.html*

12 *Op cit*, Dorr

13 *Op cit*, Dorr

14 Office of the Comptroller of the Currency, "Third Party Relationships," OCC Bulletin 2013-29, US Department of the Treasury, 30 October 2013, *https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html*