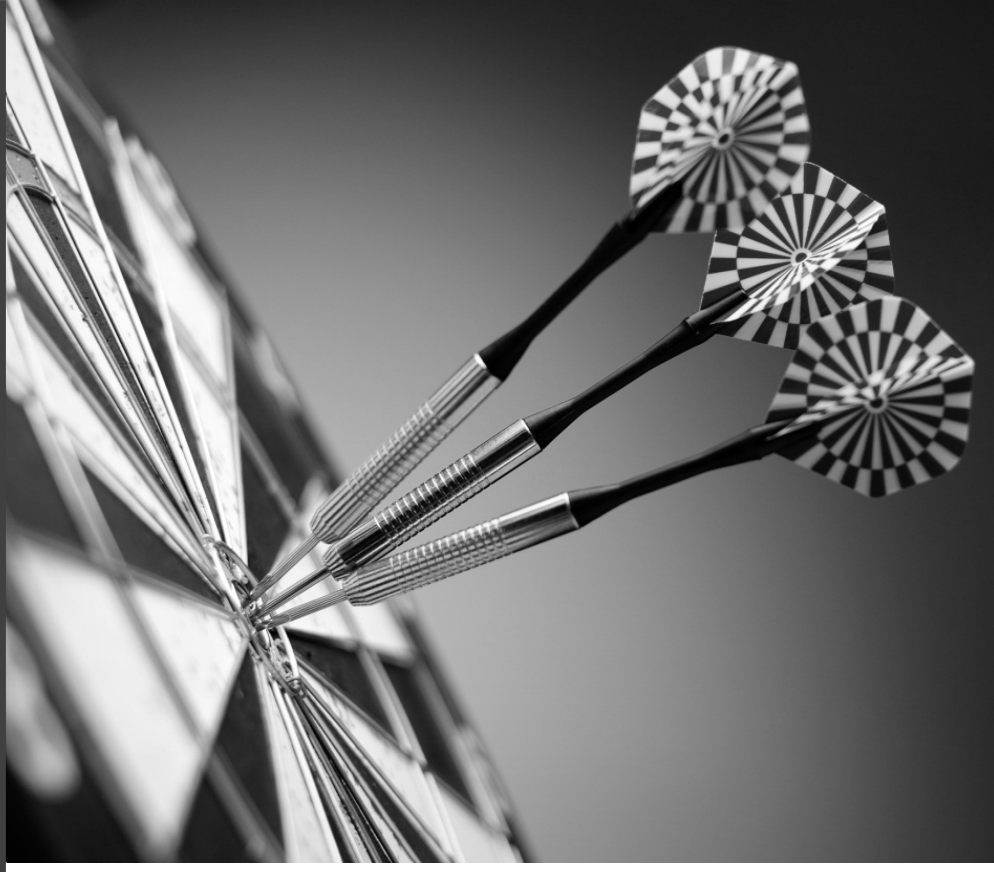
IT Insights

Managing Third Party Technology Risk



According to a recent study by the Institute of Internal Auditors, more than 65 percent of organizations “rely heavily” on third parties, yet most allocate less than 20 percent of their internal resources for assessing third-party risk.

FROM FULL OUTSOURCING of complex functions like data processing or component manufacturing to small contracts with local service providers and suppliers, companies of all shapes and sizes rely heavily on third parties.

The savings and operational efficiencies of using third parties are often readily apparent. But relying on them also means expanding your potential risks. Understanding and addressing these risks as part of a broader risk management approach is essential in order to minimize exposure to financial losses, regulatory noncompliance and reputational damage.

UNDERSTANDING THIRD-PARTY RISK

Third-party risk isn’t limited to multinational companies that outsource major business functions to offshore vendors. The fact is that most companies interact with third parties on a regular basis as part of the normal course of business. Even small companies rely on them for everything from IT support to licensed distribution. But as the number of third parties increases, so does the potential risk universe.

weaver
Assurance · Tax · Advisory

Proper due diligence before entering into a new third-party contract is just a start. Just like enterprise risks, third-party risk should be regularly and proactively managed throughout the life of a vendor relationship. This can mean leveraging internal audit, finance, legal and—in many cases—independent auditors.

NOT ALL THIRD PARTIES POSE AN EQUAL RISK

UNDERSTANDING WHICH THIRD PARTIES pose the greatest risk at any given point in time is essential for maximizing the impact of your risk management efforts.

Given most organization's dependence on data—much of which is proprietary or confidential—any third party with access to sensitive or significant information can pose a risk.

However, as with other categories of potential risk, there are degrees and hierarchies to consider. For most organizations, these parameters will change over time, depending on factors ranging from economic shifts to changes in the - regulatory environment to evolving strategic initiatives.

While not an exhaustive list, the types of third parties that typically pose a higher degree of risk to your organization include service organizations such as:

- Cloud computing/on-demand computing
- Software-as-a-Service (SaaS)
- Web design, development and hosting
- Internet service providers (ISPs)
- Credit card processing platforms
- Online order fulfillment
- Rebate processing (online and mail)
- Application service providers (ASPs)
- Data center and co-Location providers
- HR and payroll services
- Tax credit and empowerment services
- Third-party administrators (TPAs)
- Print and mail services
- Third-party logistics (3PL) services
- Accounts receivable processing and debt collection services
- Professional services (legal, accounting, etc.)

weaver
Assurance · Tax · Advisory

WHAT'S AT STAKE?

THE IMPACT OF THIRD-PARTY RISK ISN'T LIMITED TO the particular business function for which services have been contracted. In fact, the implications often extend throughout your entire organization, often with a snowball effect. For example, a network breach at a third-party service provider could result not only in loss of intellectual property, but loss of revenue, customers and reputation.

What's more, from the Office of the Inspector General to the Federal Trade Commission and the Consumer Finance Protection Bureau, regulators across the board have begun to focus on third-party risk. Organizations are increasingly expected to proactively identify and manage third-party risks and provide assurance that their service providers are compliant with a host of regulations. In addition, under provisions of U.S. Foreign Corrupt Practices Act (FCPA), U.S. corporations may even be held liable when they fail to prevent a wide range of crime, corruption and fraud from being committed by service providers operating in foreign countries.

Financial

Loss of revenue, issues with mark-up and rebates, tariffs, overpayment to vendors, regulatory fines

Operations

Supply chain issues, disruption of the business, contract disputes

Reputation & Integrity

Fraud, loss of customer or investor confidence, conflicts of interest, brand erosion, regulatory non-compliance

Technology & Information

Loss of intellectual property and trade secrets, exposure of confidential client data, loss of data integrity, denial of service/ system availability

weaver
Assurance · Tax · Advisory

Third-Party Risk Management Checklist

- Ownership is clearly defined
- Third-party risk is a component of the organization's overall enterprise risk management program.
- A full inventory of third-party relationships and agreements has been performed
- Third-party relationships have been risk rated and ranked accordingly
- Adequate resources—whether internal or external—have been dedicated to the third-party risk management process
- Third-party risks are assessed on an ongoing basis, such as prior to renewal of contracts and agreements

MANAGING THIRD-PARTY RISK

UNFORTUNATELY, MOST ORGANIZATIONS ARE REACTIVE, dealing with third-party risk only after issues occur, rather than managing and monitoring it proactively. This not only decreases the effectiveness of mitigation efforts, but increases overall exposure. Indeed, when it comes to proactively managing third-party risk, the consensus among industry professionals is that organizations must simply start somewhere.

Ultimately, third-party risk management is a moving target and an ongoing process—not a discrete, one-time event. As with any risk management program, it will take time for your approach to mature. To remain successful, you will need to adapt and evolve your approach as the information you have available improves, and as your needs and objectives change over time. There are, however, standard tools and best practices professionals regularly leverage when establishing a third-party risk management program, including ISO 27001:2013, COBIT 5, and NIST SP 800-53. Such tools can offer a high-level roadmap of where to begin.

Who Owns Third-Party Risk?

One of the challenges organizations face for effectively addressing third-party risk is determining ownership of the process. Just as responsibility for third-party relationships is often spread among several departments, so too is ownership of third-party risk: some aspects may be the responsibility of risk managers, while others may be the purview of internal auditors or compliance managers. An effective, holistic approach requires a coordinated effort that includes:

- Top-down executive leadership and oversight
- A defined and empowered ownership group
- Cross-functional input from key stakeholders across the organization (internal audit, legal, finance, compliance, procurement, etc.)

Any third party with access to your network or data can pose a serious risk.

In 2013, an HVAC contractor's network access was exploited to plant malware on a major retailer's network. The breach resulted in 40 million stolen credit card numbers; the aftermath included a 46 percent drop in 4th quarter profits and the removal of the company's CEO—not to mention the lasting reputation damage.

weaver
Assurance · Tax · Advisory

A Risk-Based Framework: Identify, Assess, Respond

RISK IDENTIFICATION

In order to identify third-party risks, organizations must have a clear understanding of their current third-party relationships. This starts with compiling a complete inventory of third parties. It may sound simple, but it can be a daunting task, particularly for large organizations that may have thousands or tens of thousands, of supplier relationships of all shapes and sizes.

Once an inventory of relevant third parties is created, organizations should catalogue the profiles for each vendor. In doing so, many organizations focus solely on quantitative considerations such as annual spend or transaction volume. However, best practices dictate that you should also catalogue and monitor other qualitative factors that often play a role when assessing risk. These factors may include:

- Financial stability
- Control environment
- Technology environment and sophistication
- Internal system linkages and dependencies
- Access to sensitive data or intellectual property
- Criticality in supply chain
- Geographical locations
- Operational characteristics
- Regulatory/compliance interaction

The biggest challenge to developing a vendor profile for risk identification is that most organizations simply don't have the data needed to do so. In most cases, a process will have to be created to obtain it.

RISK ASSESSMENT

Once third parties have been identified and profiled, it is time to assess the risks they may pose to your organization. This risk assessment should consider the likelihood of exposure and potential impact for financial, regulatory, operational or reputational factors should an issue (for example, a security breach) occur. Such factors should be tailored to your organization, and will likely evolve over time as regulatory, technology, market or operational changes dictate.

From the risk assessment, a comprehensive third-party risk rating will emerge, based on each identified risk factor. Additional investigations may also be warranted, prompting the need for a more detailed description of specific risks relating to critical service providers and vendors.

It is important to remember that there is no one-size-fits-all approach for assessing third-party risk. Assessments should be tailored to your organization's regulatory landscape, line of business, strategic initiatives and operational structure. What's more, the assessment approach should evolve as your third-party risk management maturity increases.

RISK RESPONSE

Once your third-party relationships have been assessed and rated—for example, as critical, high, medium or low—you must respond. Typically, there are four response alternatives: mitigate, ignore, share or avoid.

When deciding how to respond to a risk, you must evaluate the costs and benefits of each potential risk response, and analyze which response will result in a tolerable residual risk level. The ultimate decision will be based on your organization's risk appetite, risk tolerance and overall risk portfolio. In those instances when mitigation is the appropriate response, mitigating controls could include:

- Renegotiating contracts to include liability and penalties, right-to-audit clauses, or limits on access to sensitive information
- Implementing additional management oversight or monitoring
- Requiring added assurance measures, such as site visits or independent third-party audits

THE SPECTRUM OF THIRD-PARTY AUDITS

ORGANIZATIONS THAT OPT TO MITIGATE RISK through added assurance measures will find that there is a wide spectrum of options, each providing varying levels of assurance. When relying on third-party audits to mitigate identified risk, it is essential that you confirm not only the purpose and scope of each type of assessment, but also the type of resulting reports.

Assurance Type	Focus	North America	Global
Self-Assessment	Security & Privacy	Safe Harbor, HIPAA, FISMA, GLBA	EU Data Privacy Directive
Certification	Security & Privacy	PCI, FedRAMP, CSA STAR	PCI, ISO 27001, ISO 20000 (ITIL)
Attestation	Financial Reporting Risk	SOC 1: SSAE16 (US), CSAE 3416 (Canada)	SOC 1: ISAE 3402
	Technology Risk: Security, Availability, Processing Integrity, Confidentiality and Privacy	SOC 2: Trust Services Principles and AT 101 (US) CSA STAR Attestation	SOC 2: ISAE 3000

In the table above, the level of assurance increases from top to bottom:

- **Self-assessment** by the supplier provides the least assurance. In addition to inherent bias, suppliers often lack the knowledge and processes necessary to effectively evaluate their own organizations.
- **Certification** is typically a more rigorous process than self-assessment, requiring evidence of compliance with certain requirements or standards. However, certification is often a one-time compliance "snapshot" focused on a particular regulation, and regular monitoring or recertification may not be required. As such, it provides only a moderate level of assurance.
- **Attestation** provides the highest degree of assurance, as it requires an independent review of processes, technology and controls, typically covering a period of six months to one year.

The CFPB fined a major credit card company $210 million to settle charges of deceptive marketing practices on the part of some of the company's suppliers. Yet another major credit card company agreed to pay $112 million to settle a CFPB action.

Service Organization Control (SOC) Reporting

One of the most common—and comprehensive—attestations is a report on Service Organization Controls (SOC). Adopted by the American Institute of Certified Public Accountants (AICPA) as a replacement for the SAS70 framework, the SOC framework and reports are based on technical standards of Statement on Standards for Attestation Engagements (SSAE No. 10 or 16, depending on which report type). There are three types of SOC reports:

SOC 1: Reporting on Controls at a Service Organization

- Area of Focus: Internal controls over financial reporting
- Report Audience: Restricted to management, user entities and user auditors

SOC 2: Reporting on Controls at a Service Organization Relevant to One or More Trust Services Principles

- Area of Focus: Controls at a service organization relevant to security, availability, processing integrity confidentiality, and/or privacy
- Report Audience: Restricted to management, user entities, user auditors, regulators, and prospective users

SOC 3: Trust Services Report for a Service Organization

- Area of Focus: Controls at a service organization relevant to security, availability, processing integrity confidentiality, and privacy
- Report Audience: Intended for general use and can be distributed publicly or posted on their website

An SOC examination can only be performed by an independent certified public accountant (CPA) or CPA firm, though firms may utilize non-CPA subject matter experts (e.g. security consultants) as part of the audit team. Individuals or firms must adhere to strict professional standards set forth by the AICPA; in most jurisdictions, CPA firms that issue SOC reports are required to undergo peer reviews to evaluate and report on their quality control system. The results of the peer review process are reported to state licensing boards and the AICPA.

Choosing an Auditor

Many organizations will find that critical third-party providers have not undergone an SOC examination. Encouraging—or even requiring—those providers to engage a service auditor can be an essential component of your larger third-party risk management approach.

Key factors for third parties selecting a CPA firm to provide SOC services include:

- **SOC Experience.** Given the detailed and specific requirements of SOC examinations, organizations should select a firm with a proven track record.
- **Industry Experience.** Operational issues and risks can vary from one industry to the next. The more a service auditor understands about your provider's industry, the more effective the examination will be.
- **Resource Experience.** SOC audits require highly experienced project management, technology and security professionals, as well as those experienced in auditing controls and processes.

Key Considerations for Evaluating SOC Reports

After a third party has had an SOC examination, it's important to keep several key considerations in mind when reviewing the resulting report, including:

- Was the scope of the examination relevant to your organization's risk with that third party?
- Does the report address the specific services and locations used?
- Is the time period covered aligned with the time period of concern?
- Was the auditor's report qualified or unqualified?
- What testing exceptions were identified, and how do they relate to the risks that your organization has with that third party?

It is also essential that the third party has identified complementary user entity controls—controls the third party is communicating must be in place on the user side. Understanding these controls, and their relevance for managing specific risks associated with each service provider, is crucial to a comprehensive and effective third-party risk management process.

IN SUMMARY: YOU CAN'T OUTSOURCE RISK

AS MARKET INFLUENCES, TECHNOLOGY AND THE GLOBAL ECONOMY dictate the growing use of third parties to provide a wide array of business services and a mechanism for outsourcing of key business functions, organizations expand considerations of risk to include these third parties. The organizations most successful at addressing third-party risk are those that define clear ownership, incorporate third-party risk management into part of a larger risk management program, and evolve their approach and program over time. Organizations that ignore third-party risks open themselves to exposure on several fronts, including financial, legal, regulatory and reputational.

From the retail industry to technology to oil & gas; from small contractors with network access to global marketing providers in charge of your corporate messaging; the reality is clear: you can shift tasks and functions to a third party, but you can never outsource your risk.

weaver
Assurance · Tax · Advisory

ABOUT WEAVER

THE LARGEST FIRM BASED IN THE SOUTHWEST U.S., Weaver has more than 500 people working through operations in Texas, California, Colorado and Connecticut. We have employees from more than 16 countries, including China, France, Serbia, Zimbabwe and many more, and provide services internationally through independent membership in Baker Tilly International.

Weaver brings the rare and valuable viewpoint of a CPA firm with a dedicated, standalone IT Advisory Services practice. We understand the big picture and the larger organizational strategies of our clients, and we are accustomed to evaluating and optimizing business and IT processes for the greatest efficiency and productivity.

We approach IT Advisory Services with a holistic perspective: a keen understanding of overall organizational performance and the ways in which IT systems contribute to that performance. We see these information systems as part of the strategic whole, rather than isolated technological pieces.

Weaver helps clients thrive in an era of increasing regulatory scrutiny and calls for transparency, balancing the needs of creating effective and efficient systems with an auditor's eye for detail and an unfailing commitment to quality and IT security.

Visit Weaver.com to learn more.

Contact Us

Brian Thomas, CISA, CISSP
Partner, IT Advisory Services
Phone: 832.320.3280
Email: brian.thomas@weaver.com

weaver
Assurance · Tax · Advisory