OPTIV

THE FIVE STEPS TO MANAGING THIRD-PARTY RISK

White Paper

James Christiansen,
VP, Information Risk Management
Office of the CISO, Optiv

Executive Summary

The Common Story of a Third-Party Data Breach

It begins with a story in the newspaper. The company sent consumer information to a printing facility in an industrial park. The data was copied, without encryption, onto a server that could be accessed with shared ID or passwords. Thieves broke a window and stole the server. In addition, printed versions of the data were discarded but not shredded. The data contained not only names and addresses but also consumers' credit records. This breach represents the start of a very costly public relations nightmare.

While internal business activities present a level of risk, it is third-party relationships that make overall risk management especially challenging. As the example above shows, third parties may have access to sensitive data but often do not have appropriate controls in place to protect that data from security breakdowns. Failing to perform simple due diligence, as well as sending unnecessary data, cost this company millions of dollars.

Today, most organizations are outsourcing critical business operations to third parties. To remain competitive, organizations must balance risk management against the cost of mitigating third-party risk.

Common outsourced business operations that will drive up risk factors include:

- Billing
- Payroll and employee benefits
- Outsourced legal support
- Call-center operations
- Data center
- Cloud services
- Email
- Software or hardware partners
- Offshore manufacturing
- Offsite storage
- Outsourced software development

Third-Party Risk Ownership

Many organizations are unsure who should be in charge of managing third-party risk—is it a function of procurement, legal, compliance, risk management or information security? Without in-house compliance or risk management groups, or other internal risk management experts, the burden of managing third-party risk often falls to information security. However, this responsibility may be outside the team's mission and expertise. The complexity and scope of risk oversight may require information security to justify the high cost of third-party risk. The bottom line: organizations must assign ownership of third-party risk to a qualified team or external group, and then provide the resources and priority to accomplish the task.

What is Information Risk?

To better control third-party risk, it's critical to understand the fundamentals of information risk management, which is a function of the following:

- Inherent risk is the exposure from a third-party relationship. Inherent risk is the sum of relationship risk and business profile risk.[1]
- Mitigating controls are actions or steps that lower inherent risk.
- Residual risk is the remaining risk after applying the mitigating controls.

In other words:

Inherent Risk – Mitigating Controls = RESIDUAL RISK

Seven Types of Third-Party Risk

Third parties now provide many of the strategic functions previously conducted inside the walls of organizations. Most companies have hundreds if not thousands of third-party suppliers and partners. Regardless of the type of third party—such as billing, records management, cloud storage or OEM—these relationships and the services they provide create some type of risk to the organization. In many recent cases, supposedly low-risk third parties have presented the greatest vulnerability to security. Risk is an ever-moving, ever-evolving target that can take on many forms, including:

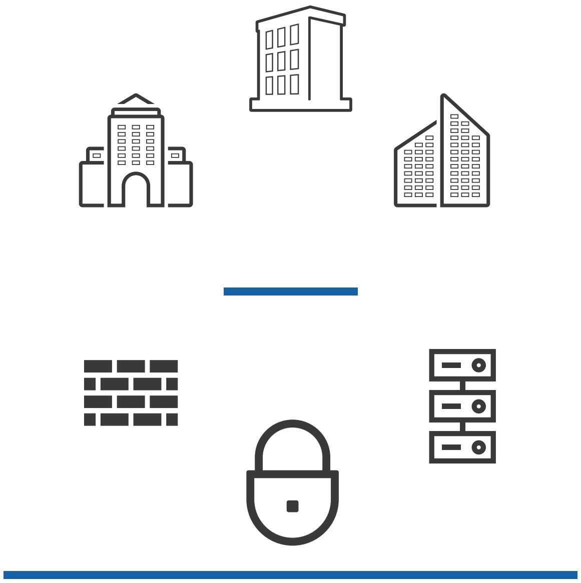
- **Strategic risk.** Organizations that rely on third parties to provide their primary goods or services may go out of business or sustain substantial losses when the third party fails to deliver. For example, OEMs that rely on a core technology of another company to develop or deliver its own product.
- **Reputational risk**. Negative public opinion poses the most expensive and difficult risk—rebuilding customer trust can take years. Several well-known breaches occurred because of a third party, but it is the primary organization that retains negative customer mindshare.
- **Operational risk.** To save costs and simplify operations, many organizations outsource critical services or functionality, such as e-mail or call centers. When these fail, business could come to a standstill.
- **Transactional risk.** This is a risk that reduces ability to deliver service. A retailer suffering from a distributed denial-of-service

[1] Reputational risk examines the type of service a third party provides, and how strategic that service is to the company. Business profile risk focuses on who the third party is—what risk do they pose. These terms are discussed in the section, "Five Steps for Managing Third-Party Risk."

(DDoS) attack may experience downtime, resulting in lost sales and loss of consumer confidence.[2]

- **Financial risk.** Businesses are at financial risk when a third party fails to meet its service-level agreements (SLAs) or are unable to deliver its product or service.
- **Compliance risk.** Third parties that violate laws, regulations, internal policies or industry requirements (e.g., PCI Security Standards) put organizations at risk for noncompliance. The primary business may be subject to government oversight, regulatory scrutiny and fines.
- **Geopolitical risk.** Often overlooked, this type of risk occurs when the third party resides in or holds information in another country where differing political, cultural or financial concerns may prohibit or inhibit delivery. Government intervention, child-labor laws or copyright laws can impact an organization's ability to do business.

[2] See http://www.techrepublic.com/blog/smb-technologist/ddos-attacks-during-the-holiday-season-dont-be-a-victim/#.

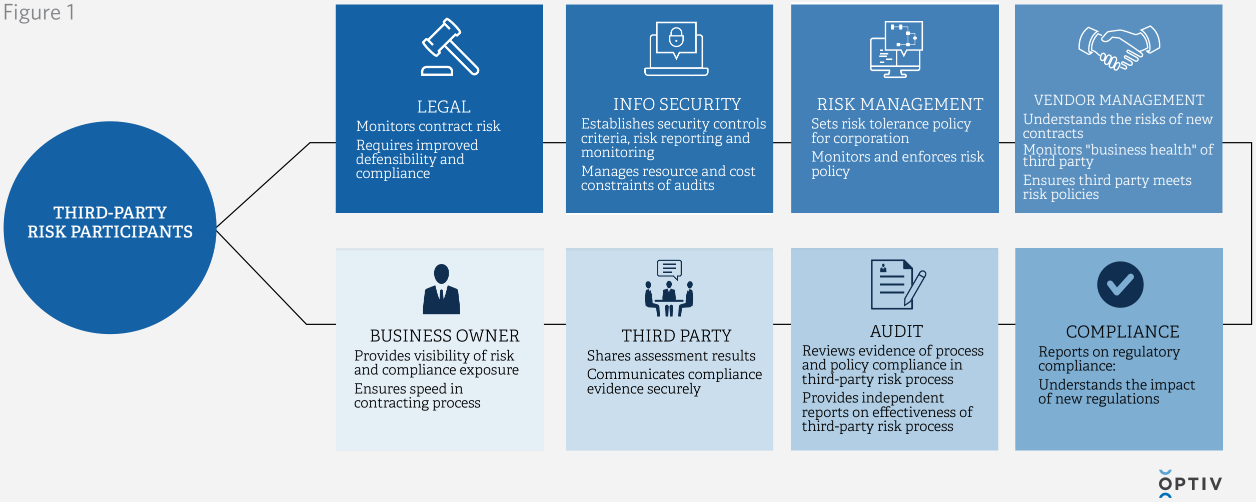


RESIDUAL RISK

The Ecosystem of Third-Party Risk

Managing the myriad of third-party risks involves a network of participants who each have a responsibility in overseeing the relationship. Internal groups—legal, IT, compliance, supply chain, procurement—must understand the performance and risk profile of a third party. The interactions among departments of the organization form an intricate ecosystem (see Figure 1). Multiply these communications by hundreds or thousands of third parties, and a complex web of connections begins to emerge. The real challenge, then, is not in managing a linear relationship between a company and a single third party, but of multiple departments within a company and its hundreds or thousands of third parties.

Figure 1



THIRD-PARTY RISK PARTICIPANTS

LEGAL
Monitors contract risk
Requires improved defensibility and compliance

INFO SECURITY
Establishes security controls criteria, risk reporting and monitoring
Manages resource and cost constraints of audits

RISK MANAGEMENT
Sets risk tolerance policy for corporation
Monitors and enforces risk policy

VENDOR MANAGEMENT
Understands the risks of new contracts
Monitors "business health" of third party
Ensures third party meets risk policies

BUSINESS OWNER
Provides visibility of risk and compliance exposure
Ensures speed in contracting process

THIRD PARTY
Shares assessment results
Communicates compliance evidence securely

AUDIT
Reviews evidence of process and policy compliance in third-party risk process
Provides independent reports on effectiveness of third-party risk process

COMPLIANCE
Reports on regulatory compliance:
Understands the impact of new regulations

- **Legal:** Identifies and monitors contract risk, and demonstrates due diligence to improve defensibility and compliance.
- **Information security:** Standardizes and automates risk reporting and monitoring to reduce the costs of audits, and enforces and validates security improvements by the third party.
- **Risk management/compliance group:** Monitors overall third-party risk and enforces obligations.
- **Relationship owner:** Has contract with the third party to deliver the product or service, and must be alert to any third-party problems—security risk, financial trouble, etc.
- **Third party management/procurement:** Manages the overall relationship with the third-party—negotiates pricing, contracts and SLAs, and ensures third-party risk assessments are done in a timely manner.

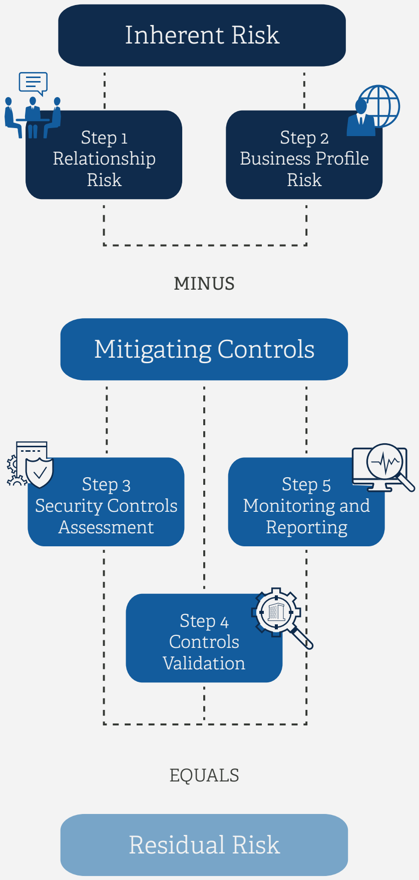
- **Auditing:** Verifies that each group completes all processes according to company policy and practice.
- **Compliance:** Performs due diligence to ensure compliance with state, federal, and industry regulations.

Five Steps for Managing Third-Party Risk

The previous sections highlight the complexity of third-party relationships, the internal owners and controls, and the various types of risk that need to be managed. Organizations struggle to find the right balance between the risk of these relationships and mitigating costs. The answer is a consistent, scalable model that can be used despite the unique variables of a particular third party.

Earlier we discussed the fundamentals of information risk management, which can be applied to third-party risk using the five-step method detailed below. Figure 2 shows the relationship between the five steps and the components of information risk management:

Figure 2



These five steps can be scaled to meet the needs of organizations with any number of third-party relationships.

1. Determine the relationship risk.

which is one of two factors for evaluating inherent risk. Relationship risk examines the type of service a third party provides, and how strategic that service is to the company. It includes the following components:

- **Strategic risk:** How significant is the monetary value of the third-party relationship?
- **Reputation risk:** Would a failure or security breach at this third-party cause embarrassment or other reputational harm to the organization?
- **Operational risk:** Would a failure of the third party to deliver impair the organization's ability to provide product or services to its customers?
- **Regulatory or contract requirements:** Do regulatory or contractual requirements prevent, restrict, or require a level of security or privacy of the data we are sharing with the third-party?
- **Geographic risk:** How do country risk factors such as lack of copyright protection or political unrest cause risk?

- **Data exposure:** Does the third party have access to sensitive financial data (e.g., M&A plans), intellectual property, technical systems information, or other confidential information about the organization?

2. Evaluate the business profile risk.

This is the second factor in determining inherent risk. Companies must understand the risk of doing business with a particular third party. This includes examining factors such as:

- **Financial status:** Is the third party a credit risk or has it declared bankruptcy?
- **Stability:** How long have they been in business?
- **Legal status:** Have they faced criminal or class-action lawsuits? Have they been breached?
- **Location:** Are they located in a high-risk country? Is there political stability?
- **Regulatory status:** How tightly regulated is their industry?

Based on the inherent risk (relationship risk and business profile risk), companies can assign a risk tier for each third party. They can perform the appropriate level of due diligence based on the amount of risk represented by that risk tier. For instance, best practices might assign a high risk to a third party that handles personal identifiable information and a low risk to a non-strategic third party with little or no access to sensitive information. While due diligence might be minimal, companies would do well to ensure common business controls are in place before signing the contract. Companies can further mitigate risk by requiring higher-risk third parties to strengthen security controls or change contract terms.

3. Perform a security controls assessment.

This assessment measures the mitigating controls put in place to protect sensitive data and systems—which lowers the inherent risk. Using a standard set of controls such as the ISO27001/2 standard will provide a structure for the controls assessment.

Companies should ask a series of questions to determine:

- What controls have been implemented?
- How effective are these controls?

For instance, a third party may have installed a data leakage prevention (DLP) solution, but may lack the people or processes to review and react appropriately. To best mitigate risk, security controls should cover three areas:

Figure 2A

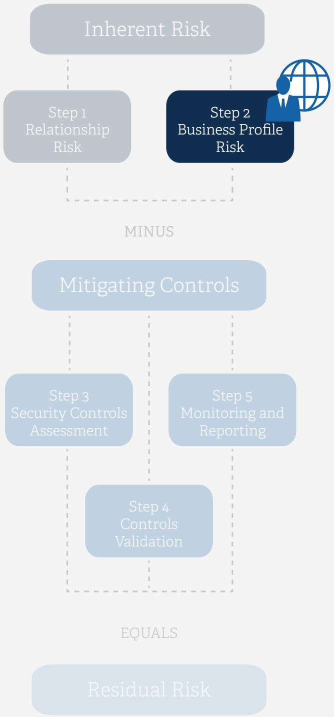
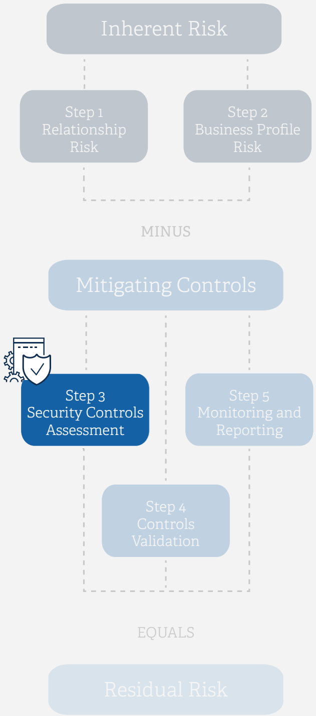

Inherent Risk
Step 1 Relationship Risk
Step 2 Business Profile Risk
MINUS
Mitigating Controls
Step 3 Security Controls Assessment
Step 5 Monitoring and Reporting
Step 4 Controls Validation
EQUALS
Residual Risk

Figure 2B


Inherent Risk
Step 1 Relationship Risk
Step 2 Business Profile Risk
MINUS
Mitigating Controls
Step 3 Security Controls Assessment
Step 5 Monitoring and Reporting
Step 4 Controls Validation
EQUALS
Residual Risk

- Prevention, such as encryption
- Detection, including intrusion detection
- Response, the ability to quickly react to an attack or alert

4. Conduct a control validation.

Companies should review evidence of the security controls in step three—they should never accept at face value the claims of a high-risk third party. This is an ongoing process, the frequency and scope of which determines the third party's risk tier. For instance, a "tier one" third party would receive an onsite visit, whereas electronic validation would suffice for less-critical providers, and a self-attest of controls for low-risk third parties.

A validation plan should cover such factors as:

- What are the controls of most concern?
- How can I verify they are functioning properly?
- What kind of evidence can they produce?
- What risk is acceptable and what is not?

Certain standards or regulations such as NIST, HIPAA, COBIT, ISO or the PCI Security Standard should be considered as the basis for validating these controls.

5. Establish a monitoring and reporting program.

This is an ongoing process for monitoring the quality of service, financial condition, risk management practices, and applicable controls of an organization's outside third parties. Insightful metrics provide executives and others an overall view of how third-party risk is being managed across the organization. These metrics include:

- Number of third parties reviewed
- What percent are compliant with the organization's security requirements
- Overall effectiveness of each third party
- Customer complaints and resolution
- Third parties' financial condition and insurance coverage
- Changes in government or industry regulations
- Trend analysis of the overall third-party risk portfolio over time

Figure 2C

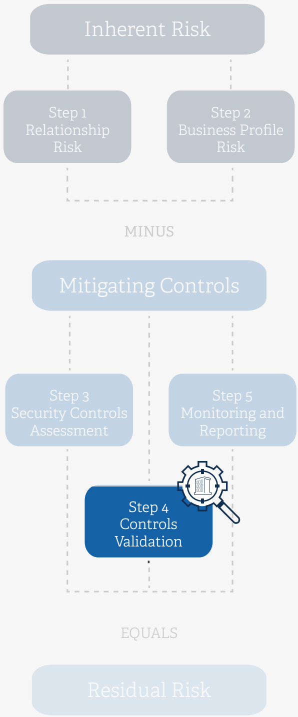
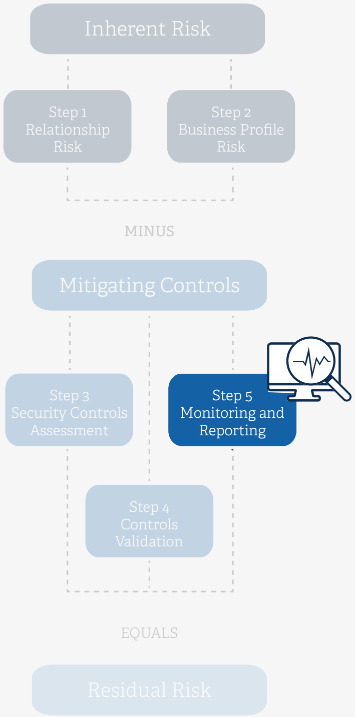

Inherent Risk
Step 1 Relationship Risk
Step 2 Business Profile Risk
MINUS
Mitigating Controls
Step 3 Security Controls Assessment
Step 5 Monitoring and Reporting
Step 4 Controls Validation
EQUALS
Residual Risk

Figure 2D


Inherent Risk
Step 1 Relationship Risk
Step 2 Business Profile Risk
MINUS
Mitigating Controls
Step 3 Security Controls Assessment
Step 5 Monitoring and Reporting
Step 4 Controls Validation
EQUALS
Residual Risk

The purpose is to provide enough information that an organization's leaders are confident with the way third-party risk is being managed across the enterprise.

Once the inherent risk has been determined, and the level of mitigating controls assessed, validated, and reported, organizations can accurately measure and best determine how to manage residual risk—or even if the relationship should be continued.

Managing Risk in the New Outsourced Economy

Third-party security breaches cost organizations hundreds of millions of dollars. Reputational harm and litigation can take years to overcome. Delayed service delivery and product disruption can affect revenue. These risks are impacting organizations daily; however, many companies rely on hundreds or thousands of outside third parties to make their business succeed. The sheer volume of these relationships creates a complex ecosystem among internal parties, and between the organization and the third parties themselves.

Organizations must understand the risk of each third party. In addition, they must continually monitor their overall third-party risk in the largely outsourced business models we see today. Several key steps that can help organizations accomplish these tasks include:

1. Assign third-party risk ownership to the appropriate department.
2. Provide sufficient resources for and prioritize third-party risk management.
3. Understand the fundamentals of information risk management.
4. Implement the five-step process for managing external risk

Finally, companies should consider implementing a third-party risk management process. Recent breaches and other security events prove that doing so can help companies find the balance between risk and cost—and thus free up organizations to focus on growth.

OPTIV

1125 17th Street, Suite 1700
Denver, CO 80202
800.574.0896
www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.