Understanding the Role of Fourth Parties in Third-Party Risk Assessment

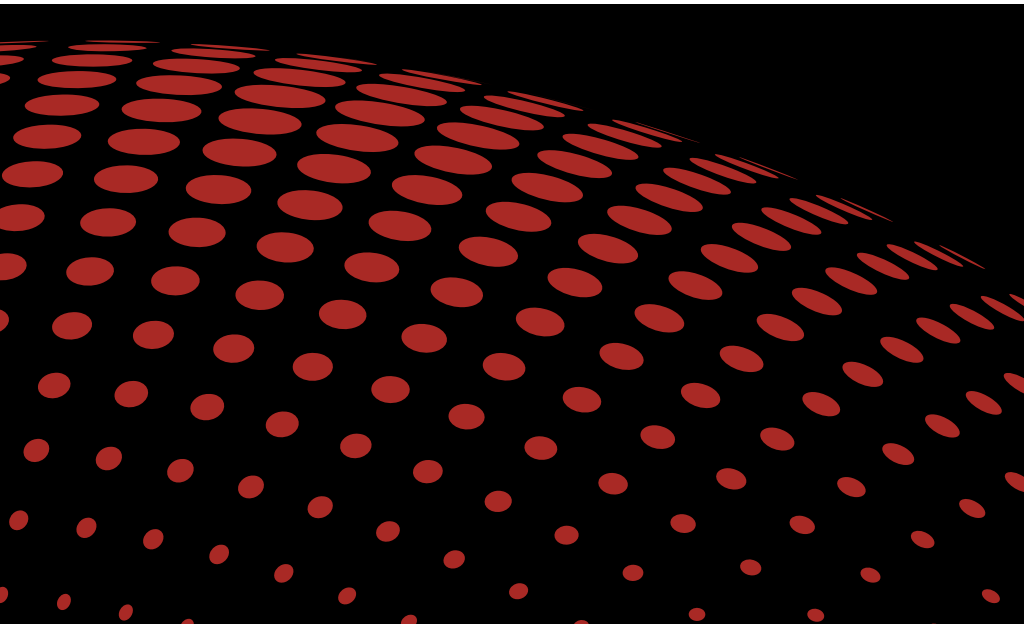


TABLE OF CONTENTS

TABLE OF CONTENTS

INTRODUCTION

Companies often rely on networks of external parties—such as manufacturers, service providers, suppliers, or consultants—to enhance their operations and benefit from outside expertise. While these partnerships are generally beneficial, they also introduce potential risks. It is crucial for companies to understand the security challenges posed by their third-party and fourth-party vendors and ensure robust security across their entire supply chain.

Unfortunately, 80% of companies worry that they lack full visibility into the security posture of their third-party partners. Gartner highlights that 30% – 40% of IT budgets are allocated to Shadow IT, which includes unapproved devices and software, adding to these risks. On average, organizations work with about 5,800 third-party vendors, as noted by Saket Modi, CEO of Safe Security, illustrating the complexity of managing fourth-party vendors.

This emphasizes the importance of fourth-party risk management, especially in industries like banking and financial services where outsourcing is common to improve efficiency. While outsourcing can enhance operations, it also introduces risks such as operational, cybersecurity, compliance, and financial threats that require diligent management.

A Security Scorecard report on the Digital Operational Resilience Act (DORA) found that 84% of financial institutions have experienced breaches through fourth-party connections. This underscores the urgent need for robust Fourth-Party Risk Management (FPRM) strategies to safeguard business continuity and resilience.

CHAPTER 1

What Are the Fourth Parties?

Understanding the network of relationships your company engages in during business operations is crucial. This involves not only your direct vendors, known as third parties, which can include suppliers, distributors, or resellers, but also the vendors that your vendors rely on, known as fourth parties. Essentially, fourth parties are the subcontractors or service providers that your third-party vendors use to deliver their services to you. Recognizing these connections helps you better manage risks and ensure the security and reliability of your supply chain.

Consider the following scenario: your company outsources IT services to a third-party provider. This provider, in turn, relies on a software company—a fourth party—for a critical service component, such as a database management system. If this fourth-party software company experiences a security breach, the impact can cascade to your company. This breach could compromise the integrity and security of the database, leading to potential data loss or exposure, disrupting your IT operations, and affecting your overall business security.

Increasing Reliance on Third and Fourth Parties

Reliance on third parties has dramatically increased, particularly with the widespread adoption of cloud-based 'as-a-service' offerings. According to a report by Gartner, 60% of organizations work with more than 1,000 third parties. This extensive network naturally extends to fourth parties, who often play critical roles in the service delivery chain but remain one step removed from direct oversight.

Challenges of Managing Fourth-Party Risks

Many organizations struggle with identifying their fourth parties and understanding their roles in the service chain. This process is challenging for several reasons:

- **Lack of Direct Contact:** Companies often do not have direct relationships with fourth parties, making it difficult to gather necessary information and maintain oversight. This indirect relationship means organizations must rely on their third-party vendors to provide accurate and comprehensive details about their subcontractors.

- **Limited Transparency:** Third-party vendors may not always be transparent about their use of fourth parties or the specific roles these entities play. This lack of visibility hampers effective risk assessments and cybersecurity defense planning.

- **Complex Supply Chains:** Modern supply chains can be incredibly complex, involving multiple layers of subcontractors. Identifying and monitoring each link in this chain requires significant effort and resources, which many organizations may lack.

- **Inconsistent Data Sharing:** Even when third parties share information about their fourth parties, the data may be inconsistent or incomplete. Different vendors might use varying standards for risk assessment, making it hard to get a clear and uniform understanding of risks across the supply chain.

- **Regulatory Gaps:** Although regulations like the Federal Information Security Modernization Act, Gramm-Leach-Bliley Act, and Sarbanes-Oxley Act require organizations to monitor third-party security, they often do not emphasize the need to monitor fourth parties. This regulatory oversight can lead to complacency, with organizations focusing primarily on direct vendors and neglecting the extended supply chain.

Fourth Parties in the Regulatory Spotlight

Fourth parties are a growing concern, especially in sectors like banking and financial services. They can increase the risk of cyber-attacks, as attackers will exploit these indirect relationships to target your company. Fourth Parties expand the potential points of entry for cyber threats, making it harder to secure your IT environment. Consequently, regulators are increasingly focused on how organizations manage these extended vendor networks to ensure security and compliance.

Fourth Party Examples Across Industries

Fourth-party relationships are prevalent across various industries. In manufacturing, a company might work with a logistics firm (a third party) that depends on multiple transportation providers (fourth parties) to deliver goods. In the financial sector, a bank might use a third party for data processing, which then employs a cloud service provider as a fourth party. Understanding and managing these relationships is vital for mitigating risks and ensuring operational continuity.

CHAPTER 2

Risks Fourth Parties Introduce

Fourth parties can bring a range of risks to an organization, and it's important to understand just how varied these risks can be:

- **Operational Risks:** This type of risk refers to potential disruptions in a business's daily operations due to issues at a fourth-party level. For instance, in the manufacturing sector, if a fourth-party supplier (a subcontractor used by your direct supplier for raw materials) is forced to suspend operations due to compliance issues or other disruptions, it directly affects the manufacturing company's production timeline and operational efficiency.

- **Legal, Regulatory, and Compliance Risks:** These risks arise when a breach or failure at a fourth-party level violates legal or regulatory standards, potentially resulting in fines and legal actions. In healthcare, for example, if a fourth-party data management vendor suffers a data breach, it could compromise sensitive patient data, putting the healthcare provider at risk of violating HIPAA regulations, leading to substantial penalties and legal consequences.

- **Reputational Risks:** This risk involves damage to a company's reputation and standing with customers, which can result from incidents involving fourth parties. For example, in the financial industry, if a third-party service provider that handles data encryption and security relies on a fourth-party vendor and that fourth party experiences a breach, it can expose customer financial information. Such a security failure can damage the bank's reputation, leading to a loss of customer trust and potentially significant business losses.

- **Financial Risks:** These risks are associated with direct financial losses that can occur due to issues with fourth parties. For example, in retail, if a logistics company (a third party) relies on several smaller transportation providers (fourth parties) that face disruptions, it could result in delayed deliveries to customers, impacting sales and the retailer's financial performance. Moreover, if the fourth party's role and security measures are not clearly defined and documented, it could lead to disputes with cybersecurity insurance claims, further exacerbating financial losses.

Recognizing these risks, regulatory bodies like the U.S. Office of the Comptroller of the Currency and the European Banking Authority, along with frameworks and regulations such as the Cybersecurity Maturity Model Certification, are putting pressure on larger institutions. They're urging these companies to not just rely on third parties for protection but also to enhance their strategies to manage risks introduced by subcontractors.

CHAPTER 3

Key Considerations in Fourth-Party Risk Management

Managing fourth-party risk effectively requires a strategic approach. Here, we will focus on two crucial steps: identifying relevant fourth parties and conducting thorough due diligence on your vendors' fourth-party risk management practices.

Identifying Relevant Fourth-Party Risk

Start by determining which fourth parties are important for your risk management framework. Not all fourth parties pose the same level of risk, so it's essential to concentrate on critical ones. The SSAE 18 report simplifies this step by requiring your third-party vendors to disclose their subcontractors in their SOC reports.

To manage this effectively, you need to prioritize fourth parties based on:

- **Importance to Your Operations:** Focus on fourth parties that are crucial in delivering your products or services. A disruption here could significantly impact your revenue and business continuity.

- **Risk of Disruption:** Assess the likelihood of a security incident or service outage at a fourth party causing a chain reaction in your supply chain.

- **Data Handling:** If a fourth party accesses or processes your sensitive data, a breach could have serious legal and reputational consequences.

To identify these critical fourth parties, use the following methods:

- **Vendor Onboarding and Annual Reviews:** During onboarding and annual reviews, request a list of your vendors' critical fourth parties. Standardizing this process ensures you get consistent and complete information.

- **Concentration Risk Assessment:** Check if multiple critical vendors depend on the same fourth party. This can amplify the impact of any issues at that single fourth party.

By focusing on these key areas, you can better prioritize which fourth parties need the most attention in your risk management efforts.

Due Diligence on Fourth-Party Risk Management

Identifying critical fourth parties is just the beginning. You also need to evaluate how seriously your vendors take fourth-party risk management. Here's why this is important:

- **Evaluating Vendor Oversight:** Due diligence helps you understand how your vendors manage risks in their supply chain. Are they proactive in identifying and mitigating fourth-party risks?

- Ensuring Robust Processes: Effective risk management involves due diligence, risk assessments, and continuous monitoring of fourth parties by your vendors.

To conduct thorough due diligence, consider these techniques:

- **Dedicated Due Diligence Questions:** Include specific questions about fourth-party risk management in your vendor due diligence questionnaires. Ask about business continuity, disaster recovery plans, SOC reports, cybersecurity, and finances to ensure they meet your standards.

- **Requesting Evidence:** Ask vendors to provide proof of their fourth-party risk management policies, procedures, and risk assessment methods.
- **Engaging in Proactive Communication:** Schedule meetings with vendors to discuss their approach to managing fourth-party risk. Ask detailed questions about their risk assessment processes and mitigation strategies.

Examples of some of the key questions to ask vendors are:

- Do they have a third-party risk management program?
- How do they assess, conduct due diligence on, manage the performance of, and re-assess the risk of their vendors?
- How do they monitor vendors and handle vendor issues internally?
- Who is responsible for vendor risk management in their organization?
- Has their program been audited or formally reviewed?

By performing comprehensive due diligence, you can gain valuable insights into your vendors' commitment to managing fourth-party risk. This information is crucial for making informed decisions about vendor selection, contract negotiation, and ongoing risk management strategies.

CHAPTER 4

Mitigating Fourth-Party Risk Through Contracts

Managing fourth-party risk effectively requires more than just due diligence. One critical aspect is using strong contractual language to shape vendor behavior and mitigate potential risks associated with their fourth parties.

Contractual Clauses for Fourth-Party Risk Management

Including relevant clauses in your vendor contracts can make a significant difference. These might include terms about how your third-party vendor manages its subcontractors, with requirements for risk-based due diligence and ongoing monitoring. Consider clauses that give you the right to audit your third party and its subcontractors and ensure non-disclosure agreements (NDAs) are in place for all parties involved.

Here are some key contractual elements to consider:

- **Written Consent for Subcontracting Critical Fourth Parties:** Reserve the right to approve or reject using specific fourth parties, especially those critical to your operations or data security.

- **Data Security and Handling Requirements for Fourth Parties:** Make vendors ensure their fourth parties follow your organization's data security standards, including data encryption, access controls, and incident reporting.

- **Indemnification Clause:** Hold vendors financially liable for damages caused by a fourth-party security breach or service disruption. This encourages them to thoroughly vet their fourth parties.

- **Multi-Party NDAs for Information Sharing:** Enable secure information sharing among your organization, the vendor, and critical fourth parties, facilitating collaboration on risk management.

- **Notification Clause for Significant Fourth Parties:** Require vendors to inform you in advance before engaging significant fourth parties, allowing you to assess potential risks and provide feedback.

By incorporating these clauses, you set clear expectations for fourth-party risk management and hold vendors accountable for their oversight practices.

The Power of Contract Language

A well-crafted contract isn't a complete solution, but it's a powerful tool for managing fourth-party risk. Strong contractual language can:

- **Enforce Expectations:** Clearly communicate your expectations regarding vendor oversight of fourth-party risk, establishing a baseline for risk management practices.

- **Protect Your Organization:** Mitigate the impact of potential disruptions and financial losses caused by fourth-party incidents through contractual clauses.

Remember, contract language is most effective when combined with other risk management strategies like due diligence, ongoing monitoring, and effective vendor communication. This comprehensive approach helps safeguard your organization from the often-overlooked threats posed by fourth-party risk.

CHAPTER 5

Additional Strategies for Managing Fourth-Party Risk

Effective fourth-party risk management involves more than just identifying critical fourth parties and conducting due diligence. So, let us now explore strategies for proactive monitoring and mitigating potential risks throughout your supply chain:

Ongoing Monitoring

Initial due diligence is important, but continuous monitoring is essential to stay informed about the health and risk posture of your vendors' fourth parties. Here are some effective methods:

- ·Risk Alert Monitoring Services: Use services that track financial health, security incidents, and data breaches involving fourth parties. This helps you address potential issues before they disrupt your operations.

- Internet News Monitoring: Set up automated alerts for negative press mentions about your vendors and their significant fourth parties. This can provide early warnings of potential problems that could impact your organization.

It's important to balance effective monitoring with respecting the privacy of fourth parties by focusing on publicly available information.

Vendor Management and Communication

Maintaining open communication with your vendors is critical for effective fourth-party risk management. Key strategies include:

- **Regular Discussions:** Schedule regular discussions about fourth-party risk during vendor performance reviews to assess their ongoing efforts and identify any concerns.

- **Tracking Contract Renewals:** Keep track of contract renewal dates for your vendors' critical fourth parties. This allows you to address potential disruptions proactively if a fourth-party contract is expiring.

By fostering a collaborative relationship with your vendors, you can gain valuable insights into their fourth-party landscape and work together to mitigate potential risks.

Escalation When Vendors Lack Proper Controls

If you discover that a vendor's fourth-party risk management practices are inadequate, take the following actions:

- **Leverage Contractual Clauses:** Use clauses in your contracts related to fourth-party risk management to compel the vendor to improve their oversight practices.

- **Report to Enterprise Risk Management:** Elevate identified risks to your organization's enterprise risk management (ERM) team or risk committee to ensure senior management is aware and can take appropriate action.

- **Amend Contracts:** Consider amending existing contracts to include stricter requirements for vendor oversight of fourth-party risk management, incentivizing them to prioritize this critical aspect of supply chain security.

Early intervention is key to minimizing potential disruptions and safeguarding your organization.

Conducting Your Own Due Diligence on Fourth Parties

In rare cases, you may need to conduct your own due diligence on a critical fourth party, especially with high-risk vendors or when a vendor's oversight practices are insufficient. However, consider the following:

- **Access Limitations:** You may not have the same level of access to information or enforcement power over fourth parties as your vendors do.
- **Cost-Benefit Analysis:** Carefully weigh the costs and benefits of conducting your own due diligence.

CHAPTER 6

4th Party Risk Management in Regulated Industries

For organizations in highly regulated industries, managing fourth-party risk is crucial. While regulatory bodies may not explicitly mandate fourth-party risk management programs, they expect organizations to take a proactive approach to managing overall supply chain risk. Here's a closer look at specific considerations for regulated industries and strategies for ensuring compliance.

Regulatory Expectations

Regulators implicitly expect organizations to address fourth-party risks, even without specific regulations. Demonstrating a robust Third-Party Risk Management (TPRM) program that includes fourth-party oversight is key to compliance. Here's why:

- **Vendor Accountability:** Regulators expect you to hold your vendors accountable for managing risks within their own ecosystems, including their fourth parties.

- **Data Security and Privacy:** Regulations like GDPR and CCPA place strict requirements on data protection. When fourth parties access sensitive data, robust risk management practices are necessary.

By implementing a comprehensive TPRM program that addresses fourth-party risk, you can mitigate potential regulatory violations and ensure adherence to data security and privacy regulations.

Strategies for Compliance

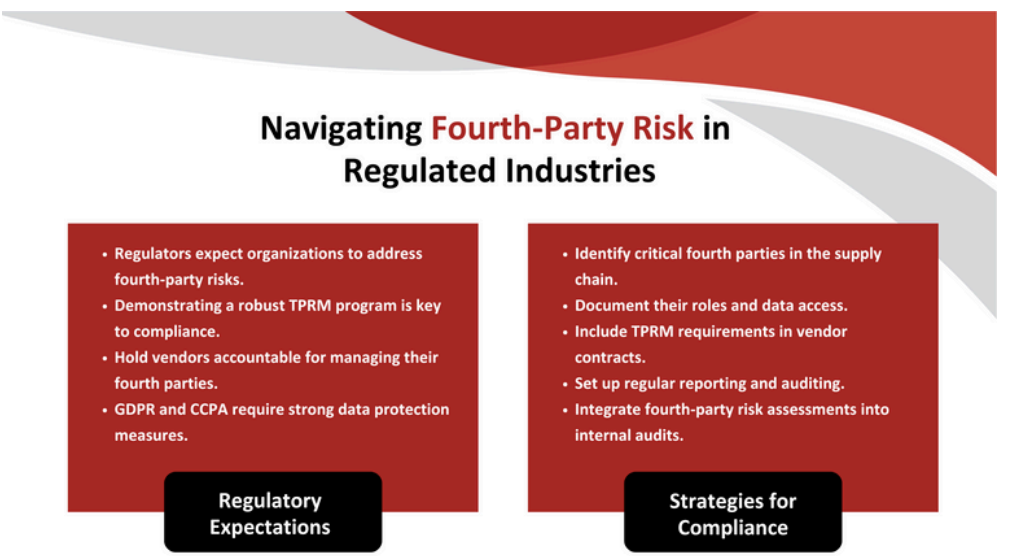
Here are practical strategies for regulated organizations to manage fourth-party risk and achieve compliance:

- **Identification and Documentation:** Proactively identify critical fourth parties within your supply chain. Keep a detailed inventory of these fourth parties and document their roles in your operations and the data they may access.

- **Contractual Obligations:** Include clauses in your vendor contracts that require them to implement their own TPRM programs. These programs should cover risk assessment, due diligence, and ongoing monitoring of their fourth parties.

- **Reporting and Auditing:** Set up regular reporting requirements for vendors about their fourth-party risk management practices. Include fourth-party risk assessments in your internal audit procedures to ensure ongoing compliance.

By following these strategies, regulated organizations can show a strong commitment to managing fourth-party risk and achieve a more comprehensive approach to overall supply chain security. This proactive approach reduces the likelihood of regulatory scrutiny and potential fines for non-compliance.



CHAPTER 7

Tips for Collaborating with Third-Party Vendors for Fourth-Party Requests

An effective fourth-party risk management framework relies on a strong partnership with your third-party vendors. Here are some tips to collaborate better with them:

- **Highlight Mutual Benefits:** Managing fourth-party risk should benefit both your organization and your third-party vendor. Show how both of you can gain from strict standards, as many risks associated with fourth parties can also affect your direct vendors.

- **Accept Your Limitations:** Understand that you won't be directly involved in managing or monitoring fourth parties. Instead, collaborate with your third-party vendors who will handle these aspects.

- **Communicate Your Concerns:** Clearly explain your concerns and needs to your third-party vendors. For instance, if you need a fourth party's SOC report, explain that it's because they have access to your organization's data, and you need to ensure its security.

Building a fourth-party risk management framework can seem challenging but focus on your third parties first. When your third-party risk management program is effective, these practices will naturally extend to your fourth parties and beyond.

CHAPTER 8

Leverage the Right Platform to Streamline 4th-Party Risk Management

Many companies are still figuring out third-party risk management, but iTech GRC, partnered with IBM OpenPages with Watson.ai, can help you tackle fourth-party risks, too.

Cybercriminals often target your supply chain, finding vulnerabilities in your vendors and their subcontractors. This can lead to serious breaches, even if the weakness is several companies away.

By partnering with iTech GRC, you get real-time insights into both your third- and fourth-party relationships, making it easier to identify and manage risks. Ready to improve your risk management? Contact us today to speak with an expert and see how iTech GRC can make a difference.

GLOSSARY

A

As-a-Service Offerings:
Cloud-based services provided to customers on a subscription basis, including Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), and Platform-as-a-Service (PaaS).

B

Business Continuity:
The ability of an organization to maintain essential functions during and after a disaster has occurred.

C

Compliance Risks:
Potential threats related to violations of laws, regulations, guidelines, and specifications relevant to an organization's operations.

Concentration Risk:
The risk of loss arising from an organization's exposure to a single counterparty or group of related counterparties that could lead to significant financial loss.

D

Data Breach:
An incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner.

Digital Operational Resilience Act (DORA):
A regulation aimed at enhancing the operational resilience of digital services within the European Union.

Due Diligence:
The investigation or exercise of care that a reasonable business or person is expected to take before entering into an agreement or contract with another party.

F

Fourth Parties:
Subcontractors or service providers that a third-party vendor relies on to deliver their services to an organization.

G

Gartner:
A leading research and advisory company that provides insights, advice, and tools for leaders in IT, finance, HR, customer service, and other areas.

Gramm-Leach-Bliley Act:
A U.S. law that requires financial

GLOSSARY

institutions to explain how they share and protect their customers' private information.

H

HIPAA (Health Insurance Portability and Accountability Act):
A U.S. law designed to provide privacy standards to protect patients' medical records and other health information.

I

Incident Reporting:
The process of documenting and reporting details of an incident, such as a security breach or service disruption, to relevant stakeholders.

Indemnification Clause:
A contractual provision in which one party agrees to compensate the other for any harm, liability, or loss arising out of the contract.

M

Mitigation Strategies:
Actions or steps taken to reduce the severity, seriousness, or painfulness of risk.

O

Operational Risks:
Risks arising from the day-to-day operations of a business, including risks related to people, systems, processes, and external events.

R

Reputational Risks:
Potential loss to an organization due to damage to its reputation, which can result from various events, such as security breaches, scandals, or poor service.

Risk Assessment:
The process of identifying, analyzing, and evaluating risk.

S

Security Breach:
An incident where unauthorized access to data, applications, services, networks, or devices is gained, resulting in information being stolen or compromised.

Service Level Agreement (SLA):
A contract between a service provider and a customer that specifies the level of service expected during its term.

GLOSSARY

SOC Report (System and Organization Controls Report):
A report issued by an independent auditor that assesses the controls in place at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy.

SSAE 18 (Statement on Standards for Attestation Engagements No. 18):
A standard used by service auditors to assess the internal controls of service organizations and issue SOC reports.

T

Third Parties:
External entities that a company engages with directly to provide products or services, including suppliers, distributors, or resellers.

V

Vendor Management:
The process of managing relationships with third-party service providers to ensure that they meet the organization's requirements and standards.

Sales Inquiries

800 960 0149
reachout@iTechGRC.com

Dallas Headquarters

16803 Dallas Parkway
Suite 300
Addison, Texas 75001

Drive Your Business Performance And Resilience