



Jul. 1, 2024

# Successful Third-Party Risk Management

Jose Meléndez

## Introduction

Third-party risk management is a critical aspect of Governance, Risk Management, and Compliance (GRC) programs. Third-party risks are associated with vendors, suppliers, and other external partners to the organization. Third-party risks can include cybersecurity risks, financial risks, reputational risks, and legal risks. Effective third-party risk management involves identifying, assessing, and mitigating these risks to ensure that the organization is protected from harm. This white paper will discuss the importance of third-party risk management, the challenges of third-party risk management, and best practices for third-party risk management.

## The Importance of Third-Party Risk Management

Third-party data breaches occur when sensitive information is exposed or compromised as a result of a security breach at an organization's associated vendor, supplier or third-party service provider and poses a significant threat to organizations. A single third-party breach can lead to significant financial losses, reputational damage, and legal liabilities. In a 2019 survey done by Deloitte, it was found that 60% of organizations had experienced a third-party breach in the past year.

These are some examples of recent data breaches as a consequence of third-party involvement

**Target data breach:** In 2013, hackers stole the credit and debit card information of 40 million customers from Target. The breach occurred when hackers gained access to Target's point-of-sale systems through a third-party vendor that provided HVAC services to Target.

**Equifax data breach:** In 2017, Equifax suffered a massive data breach in which the personal and financial information of 147 million consumers was exposed. The breach was caused by a vulnerability in a third-party web application that Equifax used to process disputes.

**Capital One data breach:** In 2019, Capital One experienced a data breach that exposed the personal and financial information of 100 million customers and applicants. The breach was caused by a vulnerability in a third-party software that Capital One used to store data on Amazon Web Services.

**Anthem data breach:** In 2015, Anthem, one of the largest health insurers in the United States, suffered a data breach in which the personal information of 78.8 million customers was exposed. The breach occurred when hackers gained

access to Anthem's systems through a third-party vendor that provided IT services to the company.

---

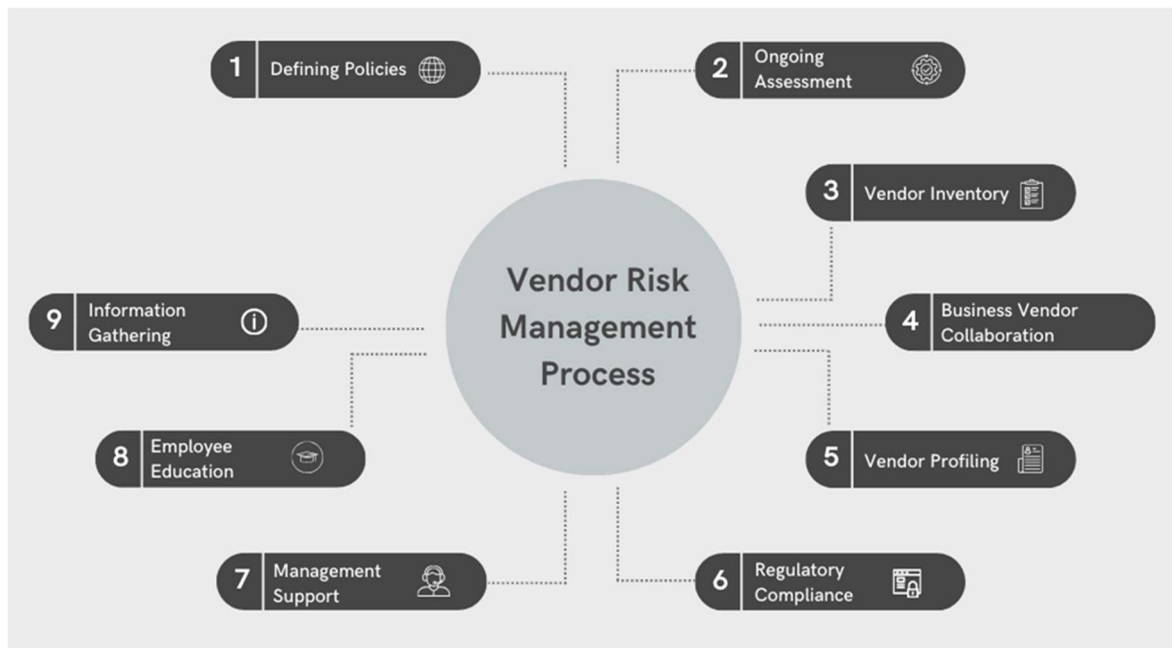
**Effective third-party risk management is an essential activity in mitigating these risks. By identifying and assessing third-party risks, organizations can implement controls to reduce the likelihood or the impact of a breach. Effective third-party risk management can also help organizations demonstrate compliance with regulations and industry standards.**

---

## Challenges of Third-Party Risk Management (TPRM)

Managing third-party risks can be a complex and challenging process. Some of the challenges of third-party risk management might include but not limited to :

**Identification:** The first step in the TPRM lifecycle is to identify potential third-



party risks. This can be done by reviewing the organization's supply chain and vendor relationships to identify vendors that pose a risk to the organization's data, systems, and operations. Identifying all third-party relationships can be challenging, particularly in large organizations with complex supply chains.

**Assessment/ Due diligence:** Before engaging with a third-party vendor, due diligence should be practiced to ensure that the vendor has appropriate security controls in place and is compliant with applicable laws, regulations, and industry

standards. Once potential risks have been identified, a risk assessment should be conducted to evaluate the risk associated with each vendor. The risk assessment should consider factors such as the vendor's security controls, financial stability, and regulatory compliance. Assessing the risks associated with third-party relationships can be challenging, particularly when the third-party reluctant or is unable to provide information.

**Remediation:** Remedying third-party risks can be challenging, particularly if the third-party is uncooperative or lacks the resources to engage their outstanding risk issues.

**Monitoring:** After a contract has been signed, ongoing monitoring should be conducted to ensure that the vendor continues to comply with the organization's policies and standards. This can include regular assessments of the vendor's security controls, its financial stability, and regulatory compliance. Monitoring third-party relationships can be challenging, particularly there is lack of transparency about their activities or processes

#### Best Practices for Third-Party Risk Management

To effectively manage third-party risks, organizations should implement the following best practices:

**Third-Party Relationship Due Diligence:** Organizations should conduct due diligence on all third-party relationships, including background checks, financial assessments, and cybersecurity assessments. The assessment process typically involves the following steps:

**Identify the third-party vendors and service providers:** The first step in the assessment process is to identify all the third-party vendors and service providers that are used by the organization.

**Develop assessment criteria:** Once the vendors have been identified, the organization should establish a methodology to assess the risks associated with each vendor. This methodology should include reviews to evaluate their reputation, financial stability, regulatory compliance, and security controls.

**Gather information:** The organization, in its methodology, should collect information from the vendor through questionnaires, interviews, and on-site visits. This information should be used to evaluate the vendor's risk profile and security posture.

**Assess the vendor's security controls:** The assessment should include a review of the vendor's security controls to ensure that they are adequate to protect the

organization's data and systems. This may include a review of the vendor's policies and procedures, access controls, network security, and physical security.

**Evaluate the vendor's compliance:** The assessment should evaluate the vendor's compliance with relevant laws, regulations, and industry standards. This may include a review of the vendor's certifications, audits, and assessments.

**Determine the vendor's risk level:** Based on the assessment criteria and information gathered, the organization should determine the risk level associated with each vendor. This information can be used to provide information for decisions related to whether to engage with a particular vendor.

**Create a remediation plan:** If any deficiencies are identified during the assessment, the organization should work with the vendor to develop a remediation plan to address the issues. The plan should include specific actions, timelines, and responsibilities.

**Monitor the vendor:** Once the assessment and remediation efforts are complete, the organization should monitor the vendor's ongoing compliance with the organization's policies, standards, and regulatory requirements. This may include regular assessments of the vendor's security controls and compliance with relevant laws and regulations risk assessment Organizations should assess the risks associated with each third-party relationship on an ongoing basis and determine the appropriate controls to mitigate those risks.

**Contract Management:** Organizations should ensure that contracts with third-party entities include have explicit, concise and appropriate language in relation to cybersecurity, data protection, and compliance matters and requirements.

**Incident Response Planning:** In the event of a security incident involving a third-party vendor, an incident response plan should be in place and activated to minimize the impact on the organization's data, systems, and operations. The Organization's plan to respond to third-party incidents, should include communication plans, escalation procedures, and remediation plans.

**Training and Continuous Improvement:** Organizations should provide training to employees on third-party risk awareness, including their identification and mitigation. Continuously reviewing and improving the organizations third-party risk management process is critical for ensuring that they remain effective and up to date.

## Conclusion

Effective third-party risk management is essential in mitigating the risks associated with third-party relationships. By identifying, assessing, and mitigating third-party risks, organizations can protect themselves from financial losses, reputational damage, and legal liabilities. However, managing third-party risks can be complex and challenging, particularly for larger organizations with complex supply chains. By implementing best practices such as third-party due diligence, risk assessment, contract management, and incident response planning, organizations can effectively manage third-party risks and support their overall GRC strategy.


## Contact Information

### Discover More with Virtual GRC

Unlock the full potential of your organization's risk management with our comprehensive white paper. Dive deep into the benefits and features of Virtual GRC, and see how we can help streamline your processes and enhance your security posture.

 [info@virtualgrc.com](mailto:info@virtualgrc.com)

 [www.virtualgrc.com](http://www.virtualgrc.com)

 +1 (123) 456-7890

[Try Our Trial Version](#): Experience the power of Virtual GRC firsthand with our free trial. No commitment, no risk.

© 2024 VirtualGRC. All rights reserved.

THIS DOCUMENT IS PROTECTED BY COPYRIGHT LAWS AND INTERNATIONAL TREATIES.

UNAUTHORIZED REPRODUCTION, DISTRIBUTION, OR USE OF THIS DOCUMENT OR ANY PART OF IT IS STRICTLY PROHIBITED. FOR PERMISSIONS OR LICENSING INFORMATION, PLEASE CONTACT US AT [CONTACT INFORMATION].

THIS DOCUMENT IS LICENSED ONLY FOR THE USE OF THE PERSON OR ENTITY TO WHOM IT IS ADDRESSED. REDISTRIBUTION OR REPRODUCTION OF THIS DOCUMENT IN ANY FORM, INCLUDING ELECTRONIC OR MECHANICAL MEANS, IS PROHIBITED WITHOUT PRIOR WRITTEN CONSENT FROM VIRTUALGRC.

VIRTUALGRC RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST ANY UNAUTHORIZED USE OF THIS DOCUMENT. FOR MORE INFORMATION ON HOW WE PROTECT OUR INTELLECTUAL PROPERTY, PLEASE VISIT <https://www.virtualgrc.com/legals/privacy-policy>