**Name of Organization**

**Third Party Risk Management**

December 2021

**Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

The (Name of Organization) Third Party Risk Management Document is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute this document to individuals on a need-to-know basis. Distribution by other individuals without prior authorization is prohibited. This document is unclassified but contains sensitive information.

**Table of Contents**

[I. Introduction and Purpose 5](#_Toc90303048)

[II. Risk Management 5](#_Toc90303049)

[Cybersecurity Risk 5](#_Toc90303050)

[Compliance Risk 6](#_Toc90303051)

[Strategic Risk 6](#_Toc90303052)

[Reputational Risk 7](#_Toc90303053)

[Operational Risk 7](#_Toc90303054)

[Transaction Risk 7](#_Toc90303055)

[Credit Risk 7](#_Toc90303056)

[III. Threats 8](#_Toc90303057)

[IV. Managing Risks 9](#_Toc90303058)

# Introduction and Purpose

This document defines requirements for establishing a Third-Party Risk Management program to minimize risk for cyber security incidents and breaches. Engaging third parties is meant to help organizations increase their productivity and efficiency, produce better products and services, employ hard-to-find qualified experts, and cut costs. All these benefits potentially come at the price of increased cybersecurity risks to you.

Minor flaws in a third-party vendor’s security and privacy routines may turn into cybersecurity weaknesses for your organization.

Third Party Risk Management is part of a mature security program and should be established well in advance of an incident or planned event. It can involve a combination of planning, resource gathering, organizing, training, and exercises.

# Risk Management

Risk management is the process of analyzing and controlling potential threats to your company’s data, finances, and operations. These risks can come from a wide range of sources including partners, customers, joint ventures, and counterparties, or vendors.

Third-Party Risk Management (TPRM) is the process of minimizing threats that might arise from a third party that provides products or services to your organization or your customers. Third-party risk management also involves controlling costs and mitigating risks to effectively manage the uncertainties and disruptions that can be associated with using an outside entity.

With security issues and cyberattacks posing dangerous threats to organizational data and information, third-party risk management programs and dealing with associated risks should be considered a top priority by leadership and the organization as a whole. The following sections outline the primary risks associated with Third Party Risk Management.

## Cybersecurity Risk

Cybersecurity risks include the potential for cyberattacks, third-party breaches, or other forms of system exposure that can be damaging to the technical infrastructure or business operations. The increasing dependency on third-party secure remote access to organization networks and global connectivity has made companies even more susceptible to cyber threats. Common threats include:

* Hacking
* Malware
* Pharming
* Phishing
* Ransomware
* Spam

## Compliance Risk

Compliance risk, also known as regulatory risk, occurs when laws, rules, or regulations are violated, or when business standards, internal policies, or procedures do not comply with local, regional, national, or international regulatory guidelines.

Regulations are set by multiple entities across the globe and can vary depending on which state, region, and business vertical an organization is conducting business in. This presents two main challenges: staying compliant, and the potential for security breaches if companies don’t adhere to regulations.

The following regulations are set forth by different regulatory bodies across the globe for various purposes, including the protection of operational, financial, personal, and healthcare data security information.

* **Texas Data Breach Reporting** – mandatory reporting of any breach which affects 250 or more Texans.
* **NERC CIP - North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)** is a set of requirements designed to secure the assets required for operating North America's bulk electric system.
* **PCI DSS (The Payment Card Industry Data Security Standard).** This is the information security standard for organizations handling branded credit cards.
* **GDPR (The General Data Protection Regulation).** This legal framework sets guidelines for the collection and processing of personal information for those living in the European Union (EU).
* **HIPAA (Health Insurance Portability and Accountability Act of 1996).** This U.S. legislation provides data privacy and security for safeguarding all medical information.
* **OCC (The Office of the Comptroller of the Currency).** This federal agency oversees the execution of laws for national banks, and functions to regulate and supervise banks in the United States.

## Strategic Risk

Strategic risk is created from failed or poor business decisions, or the inability to implement strategies consistent with the organizational goals. Third-party vendors that are not aligned with your organization’s practices may threaten operations or the ability to effectively execute business strategies and deliver services.

## Reputational Risk

Reputational risk refers to negative public opinion or customer perception that stems from the impact of irresponsible third-party practices. These include:

* Customer complaints
* Dissatisfied customers
* Interactions inconsistent with organization policies
* Security breaches resulting in the disclosure of customer information
* Violations of laws and regulations

## Operational Risk

Operational risk results from internal breaches, processes, and system failures. Third-party vendors are increasing operational risk since they can be closely tied to operational processes and business practices. Operational risks may be caused by:

* Employee error
* Failure to understand/adhere to internal policies
* Internal and external fraud or criminal activity
* System failures

## Transaction Risk

Transaction risk stems from issues with a service or product delivery, which can negatively impact your organization or your customers. Organizations are increasingly exposed to these types of risks when a third-party vendor fails to perform due to reasons such as:

* Fraud
* Human error
* Technological failure

## Credit Risk

Credit risk occurs when a third party or any creditor tied to your third-party vendor is unable to meet the contractual terms or financial agreements with an organization. To help prevent this risk, ensure that critical vendors are monitored for financial stability to know if they’re being affected in one or more of the following areas:

* Poor operational cash flow
* Regulatory implications
* Rising interest rates

# Threats

To make collaboration with third parties more secure, it is key to understand what threats they can pose to your organization’s cybersecurity. These are mainly:

* Privilege misuse — Third-party vendors may violate access privileges granted to them in various ways and for various reasons. Your subcontractor’s employees may willingly pass their credentials to others. Or, if access permissions in your network aren’t configured properly, a third-party vendor may get access to data that’s not supposed to be shared with them. Ensuring a high level of access control is especially important if your third parties have access to your company’s privileged accounts, critical assets, and sensitive information.
* Human errors — Inadvertent mistakes by subcontractor’s employees can cause just as much damage as intentional attacks. Common mistakes include accidentally deleting or sharing files and information, inputting the wrong data, and misconfiguring systems and solutions. While being unintentional, these mistakes can still lead to data leaks, service outages, and significant revenue losses.
* Data theft — Alongside unintentional data damage, there’s a high [risk of targeted data theft](https://www.ekransystem.com/en/blog/privileged-user-monitoring-best-practices) by third parties. Without a proper third-party vendor management policy in place, there’s a risk of third-party employees stealing valuable information and using it to their advantage, which could be to the detriment of your revenue and even continued operations.
* Fourth-party risks — Fourth parties or second-tier third parties are subcontractors of your subcontractors. Ensuring that your third-party vendors meet your cybersecurity requirements and follow cybersecurity best practices isn’t enough. You also need to understand how they manage their own supply chains.

An organization can effectively manage all these risks and threats by following a set of third-party vendor risk management best practices that will significantly improve your organization’s cybersecurity posture.

# Managing Risks

A systematic approach can help mitigate potential cybersecurity threats and manage risks originating from third parties. This process can cover different aspects of your company’s operations: work with sensitive data and intellectual property, access management, financial operations, and so on.

There are several international standards and commonly used frameworks that can serve as a basis for outlining your third-party risk management strategy. The following resources will prove particularly helpful:

* [National Institute of Standards and Technology (NIST) Cybersecurity Framework](https://www.nist.gov/cyberframework) (CSF)
* [NIST Special Publication 800-53](https://nvd.nist.gov/800-53)
* [ISO/IEC 27000:2018](https://www.iso.org/standard/73906.html)
* [ISO/IEC 27001](https://www.iso.org/isoiec-27001-information-security.html)
* [ISO/IEC 27002:2013](https://www.iso.org/standard/54533.html)

By analyzing the recommendations in these resources, we can summarize seven third-party security risk management best practices:

**Inventory**

An inventory of all third-party vendors and service providers is key. Next, classify them according to the level of their impact on your organization: low, medium, or high. The more critical data is exposed to a particular vendor, the higher that vendor’s possible impact on the organization.

Most attention should be paid to vendors who have a high impact on your organization’s operations and cybersecurity, as their compromise will affect you the most. Also, consider developing a framework for categorizing vendor impact and use it when starting to work with new subcontractors.

**Delineate responsibilities**

Use Service-Level Agreements (SLAs) to determine who’s responsible for what in your cooperation with a third party. Everything needs to be considered: what kinds of sensitive information your third-party vendor can access and store, what security precautions they should take to protect that data, what compliance requirements they must follow, how often they should perform audits, and so on. Think of every detail relevant to your business and make sure to reference it in your SLA.

**Establish cybersecurity policies**

Set clear cybersecurity rules for both third-party vendors and employees cooperating with them. Develop an internal policy that clarifies responsibilities of each party and outlines standard actions for different procedures and cases.

**Limiting access**

Deploy a Privileged Access Management (PAM) solution to make sure that only legitimate users can access your company’s sensitive information. This means securing critical assets with [two-factor authentication (2FA)](https://www.ekransystem.com/en/two-factor-authentication-tool) to make it harder to compromise a network even if someone’s credentials are stolen. One-time passwords and manual access approval also can help prevent attackers from entering your organizations network.

**Continuous user activity monitoring**

Continuous [monitoring of user activity](https://www.ekransystem.com/en/product/user-activity-monitoring) is a common requirement of many IT regulations, laws, and standards. By monitoring a third-party vendor’s activity within your network, it can be seen who does what with your critical assets and when they do it.

A solution that can monitor and record user sessions in a comprehensive format suitable for further auditing of your third-party vendors’ activity can be beneficial to many organizations. Reports based on the results of vendor monitoring will be helpful in passing external audits, evaluating your cybersecurity posture during internal audits, and investigating cybersecurity incidents.

**Planning for third-party incident response**

Preparing to respond to a subcontractor-related incident before it happens is important. Analyze the scope of cybersecurity threats and risks to pick those that are relevant to your organization, which allows you to develop formalized procedures for mitigating those risks.

To ensure timely detection of cybersecurity incidents, a dedicated solution to configure alerts and notifications for possible suspicious actions and events related to your subcontractor’s activity should be implemented. Responsible personnel (Incident Handling Team) should be notified in the event of a cybersecurity incident related to third parties and their names and contact information should be added to your organization Incident Response Plan (“the Plan”).

**Perform regular audits**

Perform regular audits and evaluations of all third-party vendors. Use reports from your user activity monitoring solution and incident response system to analyze the way your vendors interact with your critical systems and sensitive data.

Additionally, perform regular assessments using vendor risk management questionnaires. Having vendors fill out questionnaires will help you evaluate your vendors’ cybersecurity approaches and identify potential weaknesses in them.