graphite® Connect

Third-Party Risk Management:

An Expert Guide for Procurement Teams

As your business grows and evolves, it’s exposed to potential risks that can significantly impact your business operations and financial stability. This is especially true with external or third-party risks such as those associated with suppliers and vendors. Therefore, it’s essential to be able to define, measure, manage, and continuously monitor these threats. That’s where third-party risk management comes in.

What is the Third-Party Risk Management Process?

Risk management is the act of proactively identifying, assessing, and addressing risks affecting your organization’s assets and operations. The third-party risk management process, however, is the steps you follow to actively identify and optimize the above aspects specifically for third parties such as suppliers and vendors. Third-party risks or supplier risks are different from internal operational risks or even broader supply chain risks.

Why is Third-Party Risk Management Important in Procurement?

The third-party risk management process is a key component of the entire procurement chain since your business depends on suppliers for essential products and services. Your procurement team must anticipate and manage any potential supply chain disruptions that could impact your organization's performance. By strategically managing risks, your team of procurement and supply chain professionals can ensure you secure the needed services and products from your suppliers to maintain business continuity.

If not appropriately managed, risks can consume a significant portion of your company's resources. However, with a well-implemented risk management strategy, your organization can take calculated risks without incurring excessive costs.

Let's dive deeper into what it takes to develop a mature risk management program.

Stage 1: Define & Identify Third-Party Supplier or Vendor Risks in Procurement

The first stage in the third-party risk management process is clearly defining and identifying potential risks. Aaron Oyler, Chief Product Officer at Graphite, emphasizes the importance of acknowledging the risks' existence and pinpointing their exact nature and location: "Knowing the risks are out there is one thing, but identifying where that risk is located is quite another."

> **"Knowing the risks are out there is one thing, but identifying where that risk is located is quite another."**

Aaron Oyler

Chief Product Officer at Graphite

Understanding the Spectrum of Third-Party Risks

Third-party risk identification involves recognizing all potential hazards to your organization's assets and operations, especially those arising outside the business as is the case with vendors and suppliers. This step is crucial for laying a solid foundation for effective risk management.

- **Inherent risks** refer to the probability and impact of an adverse event without any risk management efforts.
- In contrast, **residual risks** are the risks that remain after existing risk management measures have been applied.

Categories of Supplier Risks

Various types of risks can pose a threat to your business. Examples include:

- **Financial risks** include issues like credit and liquidity risks.
- **Operational risks** encompass fraud, system failures, and other operational setbacks.
- **Strategic risks** include competitor threats and market changes.
- **Compliance risks** are associated with regulatory changes and legal compliance.

Broader Vendor Risk Perspectives

Apart from these specific categories, you should also be aware of:

1. **Core Business Risks** – These are the inherent threats to the nature of the business, including operational, financial, and strategic risks.
2. **Regulatory Risks** – These risks arise from non-compliance with industry laws and regulations.
3. **Industry-related Risks** – These stem from external factors like economic conditions, market trends, and competition.

By identifying these risks, you can better evaluate your organization's potential exposure and develop effective strategies for managing them throughout your procurement processes.

Stage 2: Measure & Prioritize Third-Party Risks in Procurement

The second stage in the third-party risk management process is meticulously measuring and prioritizing your identified risks. Here are a few tools that can help you:

Crafting a Comprehensive Register for Risks

A fundamental tool in this stage is a risk register. This crucial document should list all identified risks, their probability of occurring, their potential impact, and the procurement strategies to manage them. Each item in the register should be assigned to an owner who is responsible for actively managing it.

Enterprise Risk Console

Rank	Business Risk	Category	Likelihood	Impact	Inherent Risk	Residual Risk	Risk Thresholds
1	**Data Center Outage**	Operational Risk	Possible	Extreme	15	12	Above
2	**Interest Rates Rise on Variable Debt**	Financial Risk	Possible	Major	12	12	Within
3	**Supplier Risk: Bestsource Component Supply**	Operational Risk	Likely	Major	16	12	Above
4	**Opportunity: Changing Preferences Leading to a Decrease in Market Size**	Strategic Risk	Almost Certain	Major	20	15	Above
5	**Severe Illness for Key Executive**	Operational Risk	Likely	Major	16	9	Within
6	**CAD$ rises > than 10% against US$**	Financial Risk	Possible	Major	12	6	Within
7	**Sample Parent Risk for Roll Up Purposes**	Strategic Risk	Possible	Major	12	6	Within
8	**DDoS Attack Takes Down Production System**	Operational Risk	Likely	Major	16	10	Within
9	**Drop in Value of European Cash Reserves**	Financial Risk	Likely	Moderate	12	8	Within (Suppressed)

Utilizing a Matrix for Consistent Assessment

Leveraging a matrix can help you evaluate and rank each risk effectively. A matrix is a visual tool that assesses each threat's probability and potential impact. Assigning a score to each item on the matrix allows you to prioritize and determine which risks require immediate attention.

The matrix helps to distinguish between high-priority risks, which may require urgent attention or significant resources to manage, and lower-priority risks, which can be monitored or addressed as part of longer-term strategies.

5x5 Risk Matrix Sample

Probability \ Impact	Insignificant **1**	Minor **2**	Significant **3**	Major **4**	Severe **5**
Almost Certain **5**	5	10	15	20	Extreme 25
Likely **4**	4	8	12	Very High 16	20
Moderate **3**	3	6	Medium 9	12	15
Unlikely **2**	2	Low 4	6	8	10
Rare **1**	Very Low 1	2	3	4	5

The Importance of Prioritization

Measuring and prioritizing risks enables you to clearly focus your resources on areas with the greatest need or impact.

In summary, the measurement stage in risk management brings order and clarity to the potential chaos of risks. By systematically assessing and prioritizing each threat, your organization can develop a focused and effective response strategy so that it is ready to handle challenges as they arise.

Stage 3: Initiate Third-Party Risk Management

Once risks are identified and rated based on potential impact and likelihood, developing management strategies for each is the next step. Four risk management options exist under the TAME risk-management framework: transfer, accept, mitigate, and eliminate.

Transferring Risks

Transferring the risk involves offloading the financial consequences of the risk to a third party, such as an insurance company. When investing in a policy, the insurance company assumes all financial liabilities associated with the risk domain (legal expenses, damages awarded, and repair costs).

Accepting Risks

Accepting the risk means that your organization recognizes the potential consequences but decides to continue with the activity regardless of internal risks. If this method is chosen, remember to evaluate the risk regularly and escalate if necessary. Finally, even if you select the “do nothing” strategy, the risk domain must still have an assigned owner who can be held accountable if things go awry.

Mitigating Residual Risks

Mitigating the threat is the most common approach and involves reducing its probability and impact. That’s why it’s essential to pick a third-party risk management framework for each risk factor to mitigate risks effectively. Frameworks provide a structured approach to risk management and ensure that all relevant factors are considered. Depending on the specific risk factor, there are many frameworks available.

Some traditional cybersecurity frameworks include the National Institute of Standards and Technology (NIST), which provides a comprehensive cybersecurity framework for organizations, and the Low-Moderate-Advanced (LMA) framework, which helps organizations prioritize cybersecurity efforts based on their risk profiles.

Another one is the American Institute of Certified Public Accountants (AICPA) framework, which provides a structured approach to identifying and managing cybersecurity risks.

For privacy-related risks, some frameworks include the Service Organization Control 2 (SOC 2), which helps organizations manage risks related to protecting customer data, and the General Data Protection Regulation (GDPR), which provides a framework for risk management associated with collecting, storing, and processing personal data.

Implementing policies in your procurement processes based on these frameworks is critical to effective risk management. This structured approach helps to ensure that all relevant factors are considered, that your organization addresses the most significant risks and complies with applicable laws and regulations, while reducing the risk of damage to your company’s reputation.

Eliminating Inherent Risk

Eliminating the risk is the most radical approach to mitigate procurement risk. This typically involves abstaining from activities that could expose your organization to a particular risk. Elimination is only possible for risks like too-broad system access across your organization. Risk elimination is generally the most costly procurement strategy, though.

Stage 4: Monitor Procurement Risks

Risks are constantly changing, so it’s crucial to regularly reassess them to ensure the effectiveness of your organization’s procurement processes and risk management strategies.

Conduct Annual Risk Assessments

An annual risk assessment is essential to any robust risk management process. The first step in conducting these annual assessments is to review the list of threats identified in the risk register to ensure they’re still relevant. If any risks are no longer applicable, remove them from the list. Identify and add new risks to the list as necessary.

The Head of Risk and the Compliance Committee each play crucial roles in reviewing risk assessments. These groups oversee the risk management process to ensure an organization’s risk mitigation strategies remain effective. Findings are reported to the Board of Directors or Executive Management.

The **Probability and Impact Matrix** (mentioned above) is one tool for assessing risk. This tool helps evaluate a risk’s probability and potential impact. Each risk is rated on a scale of 1-5 for both probability and impact, and the product of the two scores becomes the overall risk score. The higher the risk score, the more critical the risk.

The **NIST Framework** (also briefly mentioned above) is another tool for assessing risk. The framework provides a structured approach to identifying and evaluating risks and guidelines for implementing effective risk management strategies. The NIST framework consists of five core functions: identify, protect, detect, respond, and recover. Each portion of the framework guides managing risks and ensures that all relevant factors are considered.

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Securities Coninuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Process	Analysis	Communications
Risk Assessment	Info Protection Process and Procedures		Mitigation	
Risk Management	Maintenance		Improvements	
Strategy	Protective Technology			

Eliminating the risk is the most radical approach to mitigate procurement risk. This typically involves abstaining from activities that could expose your organization to a particular risk. Elimination is only possible for risks like too-broad system access across your organization. Risk elimination is generally the most costly procurement strategy, though.

Internal Assessments and Remediation

Internal assessments are essential to continuously monitoring risks since they help to identify weaknesses in your organization's risk mitigation processes and any other areas that require remediation.

Remediation is the process of addressing the identified weaknesses and implementing measures to manage those risks effectively. This can include implementing new policies and procedures, investing in new technologies, using vendor management systems, and providing staff training.

The remediation process should follow the risk management frameworks you have selected. Each risk owner should ensure that the remediation process occurs and the risk is managed effectively. External inputs like regulatory requirements, market changes, and new technologies can also expose your organization to risk and should be monitored. Be sure to consider external inputs when assessing risks and implementing risk mitigation strategies.

We encourage businesses to implement a comprehensive risk management process tailored to their needs. By taking a proactive approach, businesses can protect their assets and minimize risk exposure.

Real-time supplier risk tracking is essential to any team striving for success. The Graphite platform makes it easy to track supplier performance based on the criteria that matter most to you to ensure you're getting the most value out of your spend. Regardless of the risk domains, Graphite Connect can offer your supply chain risk management teams access to live data from third-party sources, enabling them to gain valuable insights into any risks lurking in your supply chain.