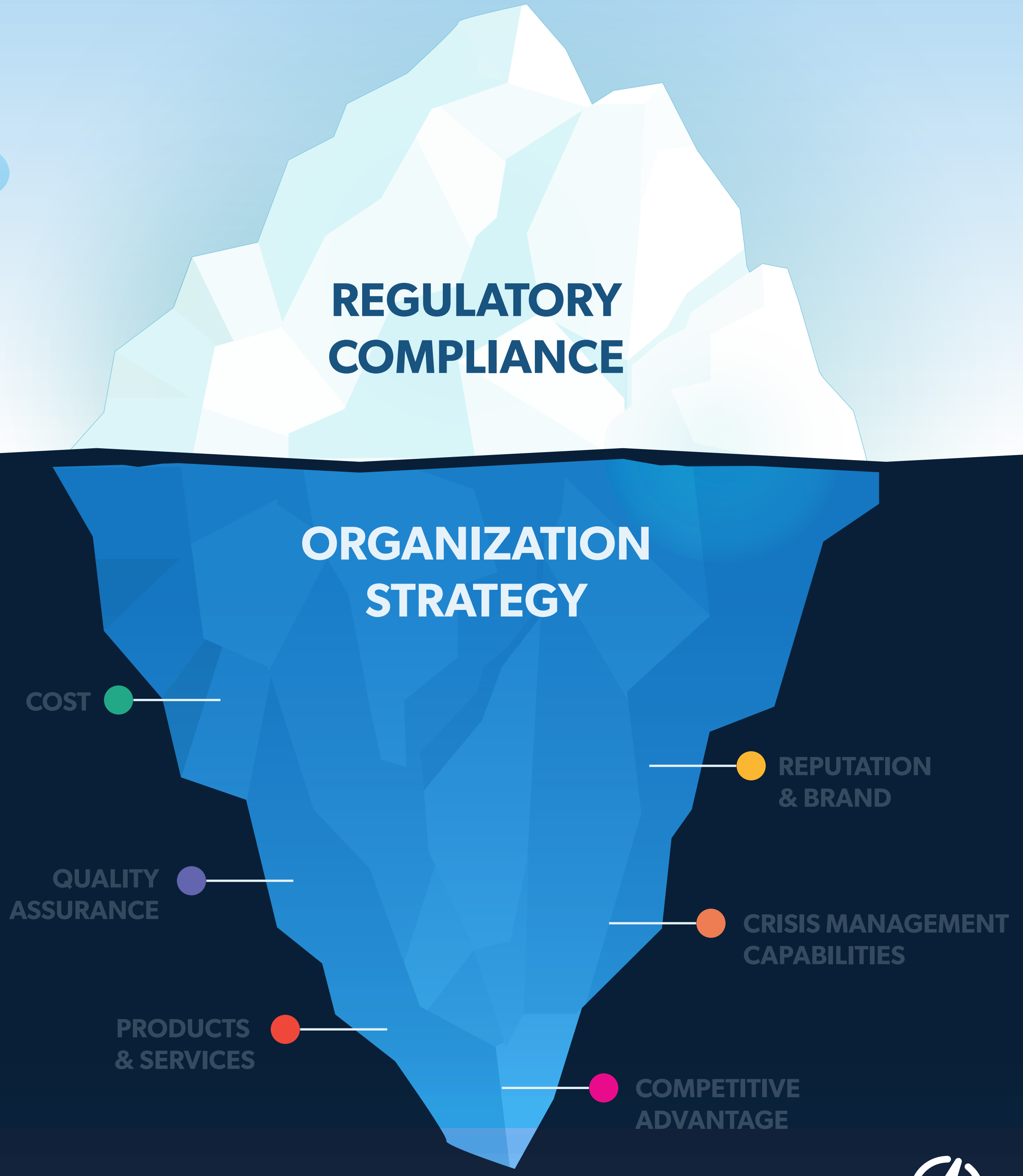
HOW THIRD-PARTY RISK MANAGEMENT ENABLES AN

Organization's Strategies



venminder

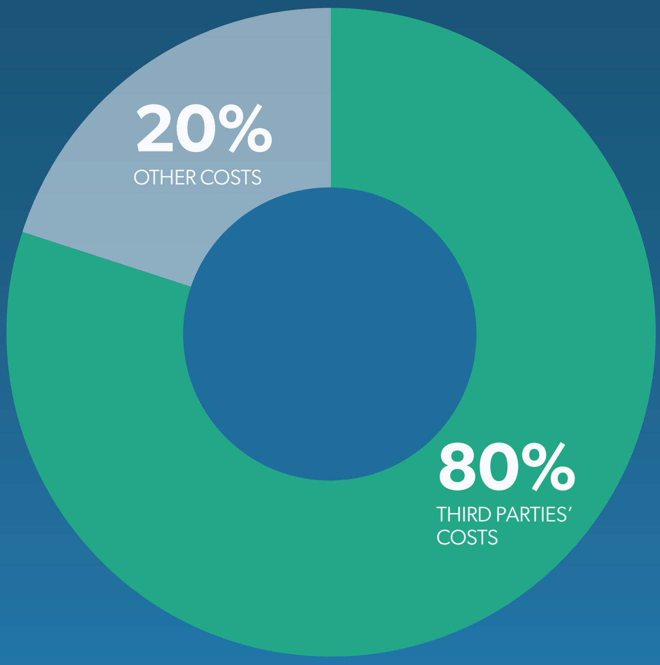
HOW THIRD-PARTY RISK MANAGEMENT ENABLES AN

Organization's Strategies

Almost every organization utilizes third-party vendors to supplement their capabilities, reduce costs, access specific expertise, augment staff or deliver additional products and services to their customers. Many organizations choose to use vendors as part of an overall business strategy. With that decision comes the necessity for third-party risk management.

The Institute of Collaborative Working estimates **that up to 80% of a business' direct and indirect operating costs can come from third parties.** Still, many organizations haven't provided the necessary attention, commitment or investment in their third-party risk management program, tools or staff. As a result, these organizations can neither confirm or fully capitalize on the anticipated benefits of using an external vendor.

Realizing the value of third-party risk management as a strategic enabler requires that organizations **look beyond the routine check-the-box requirements** of meeting regulatory requirements and reporting to senior leadership and the board. Willingness to invest in and support effective third-party risk management allows organizations to take advantage of the lesser recognized benefits third-party risk management brings to the strategic table.



Business' direct and indirect operating costs

6 Ways Third-Party Risk Management Creates **Strategic Advantages** to Organizations

1 Provides cost management and cost avoidance

Organizations want to reduce costs and improve efficiency. Third-party risk management processes are built to ensure that vendors meet expected performance. Your organization can leverage third-party risk management to identify potential cost issues before they balloon into significant problems.

Ongoing monitoring and regular risk reviews will help to:

- Prevent or reduce costly rework, regulatory fines and litigation settlements
- Provide the structure to determine when service level agreements haven't been met

2 Safeguards your reputation and brand

In the hyper-connected world of social media and a 24-hour news cycle, a single vendor incident, such as a data breach, can issue a severe blow to your organization's reputation and brand.

A third-party risk management program can lessen reputational risk through the following ways:

- Continuously examining the vendor's various risk dimensions to determine where vulnerabilities exist and how they must be mitigated before becoming a newsworthy event

- Providing regulatory compliance which includes intensive examination of cyber risk, privacy, financial health, legal risk, business continuity and disaster recovery

3 Gives your organization a framework for quality assurance

The third-party risk management due diligence process is designed to ensure that your vendor has the control environment to effectively address the risks associated with the products and services they provide to you.

Pre-contract, the execution of this process, along with ongoing monitoring will help to:

- Identify significant gaps or issues before trusting your business to a vendor
- Enable regular review and assessment of quality issues, including customer complaints
- Detect potential quality concerns before they can negatively impact your dependent processes, increase delivery time or impact your customers

4 Brings business continuity, disaster recovery and crisis management capabilities

Vendors often provide or support critical business functions.

Third-party risk management is a significant component in these areas:

- Validation that an organization’s most essential vendors can effectively resume operations after a significant business event
- Identification of vendors representing a single point of failure and referring to senior management and the board for risk acceptance and approval

5 Supports those employees responsible for vendor products and services

Many employees are hired for their expertise related to the product or service provided by their vendor. Not surprisingly, many of these individuals have no practical experience in actually managing a vendor in a third-party risk management context. First line of defense employees often struggle when vendor management is added to their duties.

Third-party risk management can be used to:

- Design and deliver vendor management training and support
- Instruct employees on how to follow procedures or navigate and use vendor management systems

6 Enhances your competitive advantage

The best way for organizations to operate more intelligently when it comes to risk is to be better prepared for it. Organizations who have a good grasp on their third-party vendor activity can avoid costly penalties, reputational damage and create a competitive advantage in their industry. You must ask if your organization is investing enough time, attention and resources to ensure your third-party risk management program can effectively support its core functions, let alone enable your business strategies.

3 Principles of Third-Party Risk Management

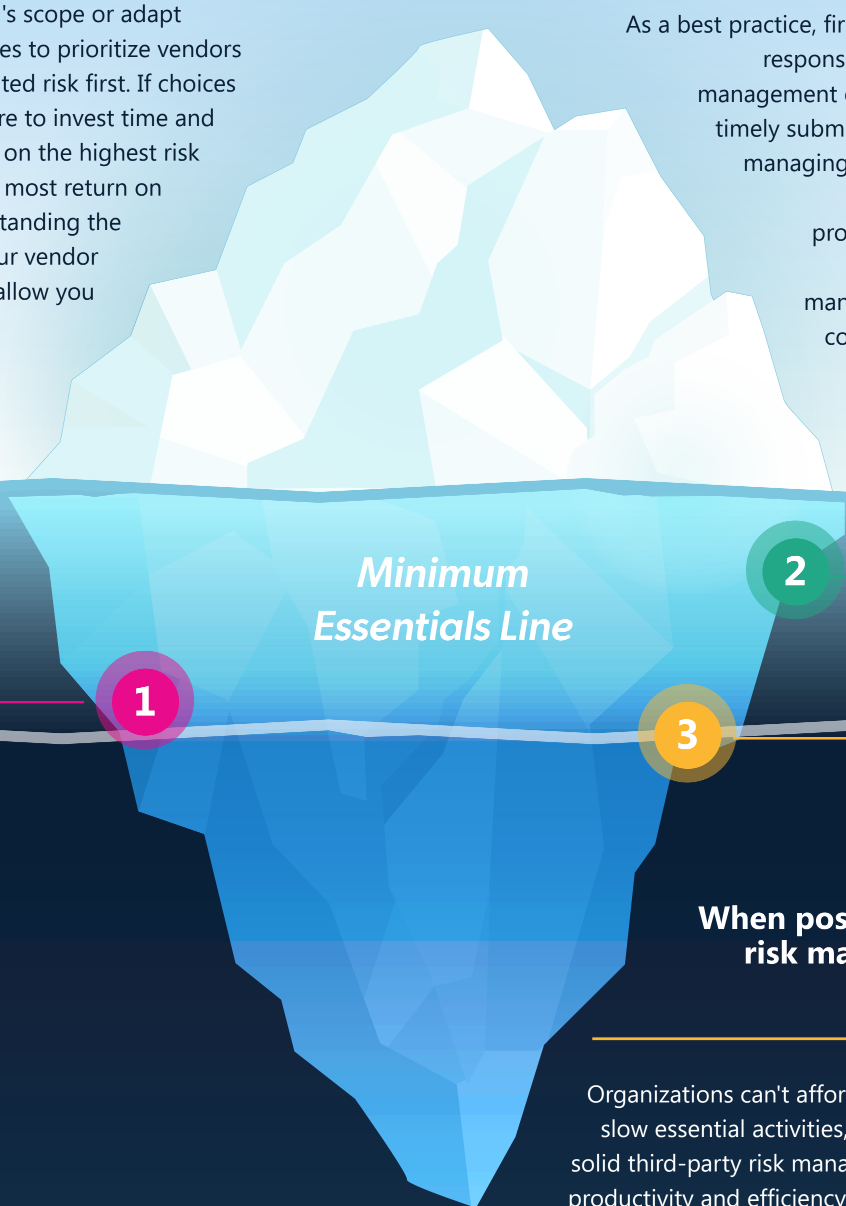
Suppose your organization isn't prepared to make additional investments in support of third-party risk management. In that case, the organization must align to three essential tenets of third-party risk management to ensure the program's success:

Be optimized to focus on highest risks.

Adjust the program's scope or adapt day-to-day processes to prioritize vendors with the most elevated risk first. If choices must be made where to invest time and resources, focusing on the highest risk vendors deliver the most return on investment. Understanding the inherent risks of your vendor inventory can also allow you to optimize your processes.

Vendor owners must be accountable for their relationships.

As a best practice, first line business owners should be responsible and accountable for the daily management of their vendors, such as ensuring timely submission of requested due diligence, managing vendor performance, addressing open issues, etc. By the first line proactively and effectively managing their vendors, the third-party risk management staff can focus on more complex and value added activities, such as managing the due diligence process to ensure shorter onboarding times.



When possible, use a third-party risk management platform to automate.

Organizations can't afford to have manual processes that slow essential activities, such as onboarding a vendor. A solid third-party risk management program enables better productivity and efficiency for understaffed third-party risk departments and their stakeholders, ensuring time is spent identifying, assessing and managing risk versus doing repetitive, time-consuming and low-value administrative activities.

To recap, many organizations believe there is untapped value in third-party risk management and that they need to better support and invest in third-party risk.

These same organizations are better positioned to realize the total value of third-party risk management if they invest in the people, processes, tools and senior leadership support necessary to do so.

Download free samples of vendor controls assessments and see how Venminder can help you reduce your third-party risk management workload.

Download Now

venminder

Manage Vendors. Mitigate Risk. **Reduce Workload.**

(888) 836-6463 | venminder.com

About Venminder

Venminder is an industry recognized leader of third-party risk management solutions. Dedicated to third-party risk, the company is the go-to partner for software, high-quality assessments on vendor controls, certified subject-matter expertise and education.

Venminder's platform provides a centralized location to execute a third-party risk management program. It enables users to store documentation, onboard a vendor, track contracts, manage SLAs, send and manage questionnaires, manage due diligence and oversight, complete risk assessments, create workflows, run reporting and more.

Assessments performed by Venminder's qualified experts, including CISSPs, CPAs, financial risk analysts, paralegals and more, are readily available in an online library. The assessments enable clients to identify possible risks and understand areas of strength on their vendors' information security and privacy standards, SOC reports, financial viability, business continuity/disaster recovery preparedness, contractual standards, regulatory compliance and more.