Steps To Establish A Vendor Risk Management Program

Managing risk of all kinds is an important part of building and maintaining a successful business.

With businesses growing increasingly interconnected by technology, and supply chains expanding to span not just territories or countries but the entire globe, effective *vendor risk management* (VRM) is especially important.

Developing a risk management process to identify and minimize risk involves addressing areas as varied as cybersecurity, regulatory compliance, vendor relationship management, and careful third-party risk assessment.

With help from the right technological tools and intelligent planning designed to address both the general challenges of vendor risk management and the process improvements specific to your business, you can build a successful vendor risk management program.

Why Vendor Risk Management Matters

The goal of VRM programs is simple: to monitor, manage, and reduce risk exposure created by relationships with third-party vendors and information (IT)

professionals.

Done properly, vendor risk management is built on a comprehensive and clear set of policies and processes that support the removal of excess additional risk and mitigation of any that already exists, including:

- Damage to a company's reputation.
- Costly legal entanglements and liabilities.
- Decisions made with incomplete or erroneous information.
- Data breaches resulting in the release of confidential information.

Thanks to globalization and widespread digital transformation, vendor risk management is about more than just vendor management in your supply chain.

To cut costs and improve both agility and profitability, many businesses are outsourcing essential business processes to third parties—part of an outsourcing market that topped $85 billion worldwide as of 2018.

In an ideal world, offloading these processes makes for a strategically valuable improvements to your own processes and reduces costs by reducing overhead and labor.

But a string of third-party vendors brings with them a commensurate amount of third-party cybersecurity risk and the potential for security breaches, cyberattacks, and other data security challenges, as well as compliance issues and reputational damage.

As a result, the information technology (IT) capabilities, information security, and cybersecurity of the vendors you choose for services as well as supplies must be as strong and reliable as your own—or better.

> *Establishing a thorough and detailed vendor selection process will provide a filter for high-risk vendors who might otherwise slip through undetected, and also allow you to refine your existing vendor list to ensure all your suppliers value security, performance, and compliance as much as you do.*

Developing a Vendor Risk Management Program

Your business needs are specific to your company and industry, but every business can develop an effective vendor risk management program by starting with a solid foundation built on a set of established best practices.

1. Begin with the Three Ps: Policies, a Program, and Procedures

Navigating the potentially treacherous waters of the third-party risk management process without first charting a course can land you on the rocks of regret pretty quickly. Decide before you begin how you will handle vendor risk assessment as part of managing vendor risk.

Ideally, you'll develop:

- **Policies**, which provide general guidance and goals for managing third-party risk exposure.
- **Program**, which provides a framework and outline useful to all stakeholders in identifying risk, addressing it, and measuring the success of corrective actions for further refinement.
- **Procedures**, which detail specific daily tasks, responsibilities, and workflows.

2. Make a Preemptive Strike against Risk with Smart Vendor Selection

Whether they're a key supplier or a service provider handling business processes, every vendor should be subjected to careful risk assessment before they're added to the supply chain or services roster.

Establishing a thorough and detailed vendor selection process will provide a filter for high-risk vendors who might otherwise slip through undetected, and also allow you to refine your existing vendor list to ensure all your suppliers value security, performance, and compliance as much as you do.

Vendor selection and review policies and procedures will vary by company, but can include:

- Taking a comprehensive inventory of all third-party suppliers. Build due diligence into your evaluation procedures for new potential vendors.
- Performing a thorough vendor risk assessment of all vendors to identify and detail cybersecurity, information security, compliance, reputational, and other data security risks each vendor creates for your business.
- Organize your vendors based on their potential risk levels, broken out by service levels. Separate those with risk levels that can be mitigated for rehabilitation, and remove those whose risk profile exceeds your company's level of acceptable risk.
- Develop a set of formalized contractual standards that can be used as a starting point in establishing or (re)assessing all third-party relationships. Such standards should make clear:
    - The responsibilities of both the vendor and your company for the life of your relationship, as well as the incentives for exceeding standards and the penalties for failing to meet them.
    - A formalized negotiation process
    - A formalized review and approval process
    - A formalized process for storing, monitoring, and modifying contracts as dictated by (re)negotiations and other changes of circumstance.
- Assign ownership of VRM and any other third-party risk management duties to the appropriate parties. Separate but collaborating teams should be established for
    - Risk management and compliance (including security controls)
    - Internal auditing
- Working with the VRM staff, build a process set that automatically analyzes risk exposure created by potential new vendors, with clear benchmarks for performance and compliance. Ideally, this system will allow for real-time evaluation of these factors for both potential and existing vendors to keep nasty surprises at bay.

  Using a comprehensive procurement solution like PLANERGY can help by automating approval workflows, providing a vendor portal connecting suppliers to your system to improve transparency, and real-time data analytics to measure essential vendor key performance indicators (KPIs).

- Creating multiple and redundant contingencies to automatically generate alerts and take action when a potential or existing third-party supplier exceeds acceptable risk levels (e.g., failure to meet contract terms and conditions, violation of industry or legal compliance, or a data breach)

3. Due Diligence is a Marathon, Not a Sprint

As it has been since the dawn of commerce, periodic due diligence is a necessary part of healthy business relationships in the 21st century.

Due diligence is made simpler by the use of automation and analysis powered by artificial intelligence.

In addition to being able to track and measure vendor performance in real time based on the KPIs you've selected, you can analyze other data that holds important information about the health and risk profile of your vendors and service providers, including:

- Financial statements, which can reveal underlying issues that can contribute to financial decline or even the collapse of a vendor's business.
- Service Organization Control (SOC) reports, which contain crucial information regarding a vendor's regulatory compliance with standards and legal and industry requirements, as well as their internal controls for achieving such compliance.
- Additional assessments your company performs to ascertain specific compliance levels, such as general risk assessments, public perception audits, and information security assessments.

Due diligence also provides an excellent opportunity to work with your suppliers in collaborative efforts at shared process improvements, creating a mutually beneficial relationship that brings greater efficiency throughout the procure-to-pay (P2P) process.

Communication and collaboration can help you turn your best vendors into strategic business partners for shared success.

4. Develop a Robust Internal Audit Process

In addition to tracking the performance and compliance of your vendors, turning

the lens on your own controls not only helps you identify areas in need of improvement, but provides clear, clean data that streamlines external audits and minimizes the risk of negative fallout from non-compliance.

As with due diligence, internal audits are greatly simplified with support from the complete data transparency and real-time access to information provided by a comprehensive, cloud-based procurement solution that includes deep data analytics.

Measuring your own IT security or Health Insurance Portability and Accountability Act (HIPPA) compliance also provides a useful frame of reference when measuring the same for your vendors.

Reporting and collaboration are also improved, since everyone involved in the process has level-appropriate access to essential information as well as the ability to generate custom reports and dashboards on demand.

The more comprehensive and clear your risk assessment, communication, and auditing processes are, the safer your business will be.

Enterprise Risk Management Program

A strategic VRM program is a key component to your company's *enterprise risk management* (ERM). ERM takes the concept behind VRM—a strong plan-driven strategy for identifying, assessing, and eliminating risk—and applies it to the company as a whole.

Managing these risks requires a nuanced and complete understanding of all the risks facing a business, including:

- Production and operational risk
- Legal, financial, and industry compliance
- Human resources management and compliance
- Internal and external controls related to the Sarbanes-Oxley Act of 2002 (SOX) in the United States.
- Organizational governance

Part of an effective ERM strategy involves investing in the best quality tools and goods, as well as purchasing insurance as a hedge against disasters both natural

and man-made.

But risk exposure and management are just as important, if not more so, to the health and longevity of a modern business in the global marketplace. That's why it's so important to develop and implement tools such as VRM.

By reducing risk with a third-party risk management program, you're directly supporting both the larger initiatives of ERM and the continuing safety, positive reputation, and productivity of your company.

Minimize Vendor Risk for Maximum Performance and Profits

You can't control the universe, but you can control how you anticipate and respond to risk.

By developing a comprehensive vendor risk management program, you can enjoy more collaborative supplier relationships, rock-solid compliance, and the transparency and responsiveness you need to anticipate and mitigate risk before it causes serious damage to your profits, production, or public reputation.

What's your goal today?

1. Use PLANERGY to manage purchasing and accounts payable

We've helped save billions of dollars for our clients through better spend management, process automation in purchasing and finance, and reducing financial risks. To discover how we can help grow your business:

- Read our case studies, client success stories, and testimonials.
- Visit our "Solutions" page to see the areas of your business we can help improve to see if we're a good fit for each other.
- Learn about us, and our long history of helping companies just like yours.

Book a Live Demo

2. Download our guide “Preparing Your AP Department For The Future”

Download a free copy of our guide to future proofing your accounts payable department. You’ll also be subscribed to our email newsletter and notified about new articles or if have something interesting to share.

download a free copy of our guide

3. Learn best practices for purchasing, finance, and more

Browse hundreds of articles, containing an amazing number of useful tools, techniques, and best practices. Many readers tell us they would have paid consultants for the advice in these articles.

Related Posts