HOW TO BUILD A BETTER VENDOR RISK ASSESSMENT: A GUIDE

CENTRL

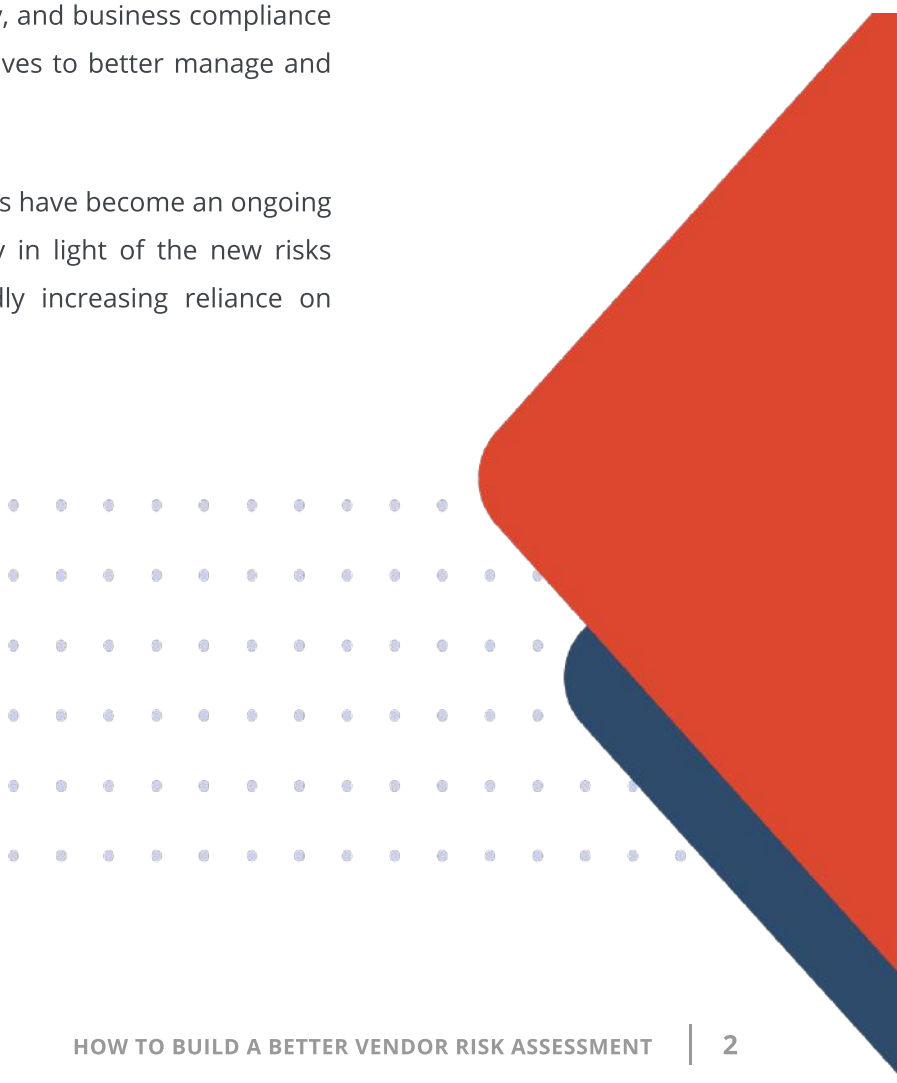
HOW TO BUILD A BETTER VENDOR RISK ASSESSMENT

Vendor Risk Management (VRM) or Third-Party Risk Management is practice concerned with identifying and mitigating risks associated with suppliers.

VRM provides enterprises with visibility into which vendors have implemented sufficient information security controls.

As enterprises experience new security, privacy, and business compliance challenges related to their suppliers, VRM evolves to better manage and mitigate these emerging risks.

As such, vendor risk management best practices have become an ongoing focus for enterprise management. Particularly in light of the new risks associated with remote work which is rapidly increasing reliance on vendors such as cloud providers.



THE BENEFITS OF VENDOR RISK MANAGEMENT SOFTWARE

A robust VRM software can help organizations to decrease the impact and likelihood of disruptive events and reduce their overall risk exposure. However, it offers far more benefits than just risk reduction.

Businesses implementing a VRM program can evaluate and onboard new vendors more efficiently, streamline their vendor management processes, and leverage these relationships to their fullest potential.

Additionally, a vendor risk program can allow organizations to monitor their vendor relationships over time, measure vendor performance, and identify new risks as they arise. Let's take a look at those different types of risks you should cover in your vendor risk assessment.

THE TYPES OF RISKS TO IDENTIFY IN YOUR VRM PROGRAM

Legal Risk

There are many legal risks associated with disclosing sensitive information to third parties. For example, if security expectations are not specified in your vendor contract, you may have no legal recourse if your vendor compromises your data.

Compliance Risk

Compliance risk is a third-party risk that can lead to an organization violating a particular law, regulation, or contractual obligation (usually known as compliance requirements), either intentionally or unintentionally.

Reputational Risk

Third-party vendor risk management includes risk to your reputation. For example, should a third-party provider of yours become embroiled in a data-privacy breach, your organization could also be held responsible.

Therefore, a series of questions should be asked at the beginning of the vendor sourcing period so that you can dispense with companies you would prefer not to work with.

Financial Risk

Financial risk is a third-party risk that can impact an organization with financial implications based on the vendor relationship.

When a supplier has a poor financial record, you will want to know that information before entering into a business partnership. Thus, checking on your suppliers financial processes and auditing mechanisms should be part of your evaluation process.

Operational Risk

Operational risk is a third-party risk associated with any negative impact a vendor can have on your own operations.

For example, if your business relies heavily on cloud providers to facilitate it's day to day operations, and a particular provider has a history of frequent outages, this vendor could represent a significant operational risk to your business.

Cyber Risk

Cybersecurity risk is an ever prevalent and increasing third-party risk. Bad actors are constantly evolving to find new ways to infiltrate corporate systems and steal, sell, or otherwise disrupt their information systems and confidential data.

To properly combat this risk, your organization needs to assess the cyber risks associated with a vendor and evaluate the security controls they have (or don't have) to assess how high of a risk they are.

So, how can you be sure you properly identify and mitigate your third-party vendor risks? It all starts with your vendor risk assessment.

HOW TO ESTABLISH BETTER RISK ASSESSMENTS THAT IMPROVE YOUR VRM PROGRAM

As your company evolves and new suppliers enter the market, your risk management program must be more thorough in evaluating each scenario that may arise.

A supplier evaluation program will always be more effective to the extent that more risks can be identified and eliminated.

Improving the quality of your evaluation methodology directly impacts the efficiency of your VRM program and the accuracy of the information you collect on your suppliers.

So, how do you build better vendor risk assessments as your VRM program evolves? Consider these four core objectives.

The Quality of the Program

This refers to everything from resourcing, communication, and repeatability.

Whether it's been a year since you launched your VRM program or five years, now is the time to take stock of these qualities and how they can be improved.

Additionally, as your ability to resource your program expands, so should the scope of your assessment methodology. Stakeholders will expect to see improvement and growth if they are to continue increasing funding for the program.

At evaluation time, it's important to ask some key questions such as,

- "Did we have time to evaluate all of the service providers we'd like to evaluate?"
- "Did we succeed in resolving all of the concerns mentioned by those inspections?"

Alignment To Overall Business Needs

Business needs evolve as the business grows and service or product lines expand.

Typically, the main objective of a first-year VRM program is to complete a certain number of assessments in order to evaluate where you stand with your vendors, identify risks, and eliminate as many as possible along the way.

However, as your company grows and the scope of your product line increases, you must consider whether the vendor risk assessment is meeting your needs.

You'll need to ask yourself some of the following questions,

- "Do the criteria I've picked represent my company's specific requirements?"
- "Which of our controls apply to our vendors?"
- "Does the scope of my existing assessment adequately capture the regulatory requirements my vendors face?"
- "Have I properly addressed the unique risks associated with my vendors?"

Veracity of Controls

When you send questionnaires to new vendors or annual recertification to existing vendors, how do you verify their responses? Through evidence collection and sampling.

Typically, this evidence will be in the form of documented vendor policies that are shared with you during the assessment process. But while policy indicates intent, it doesn't necessarily guarantee the vendor is doing the things they say they are.

To validate their claims, you must sample evidence of the control performance indicated in the policy documentation.

So for example, if the vendor claims that their information systems are protected through multi-factor authentication, you'll need to test that to ensure the multi-factor authentication is actually in place and functioning properly.

Therefore, evaluation questions for your program should include:

- "Are you running tests in an effective and efficient manner?"
- Are you testing thoroughly enough to identify where the control execution risk lies? Or are you wasting resources with unnecessary testing?

Program Efficiency

You can continue to improve efficiency by searching for controls in places where your vendors as a group are consistently successful, rather than those areas where good risk management is more challenging.

This may look like limiting the complexity of recertification questionnaires for vendors who are consistently successful.

Additionally, removing redundancies and bottlenecks in processes and workflows is also critical to optimizing a vendor risk assessment program. Vendor risk management tools provide efficiency game-changes such as automation capabilities that can empower you to both standardize and streamline processes.

While many smaller companies start vendor assessments with manual methods and spreadsheets, these mechanisms aren't scalable after you've accumulated several vendors.

HOW VENDOR360 CAN HELP YOU STREAMLINE YOUR RISK ASSESSMENTS & VRM PROGRAM

Vendor360 is a sophisticated and adaptable third-party risk management tool for collecting vendor data, automating assessments, and gaining control of your vendor risk management process.

Our platform helps our client's trade vendor management overwhelm for workflow automation, questionnaire templates, recurring assessment scheduling, auto-assigning to business users, alerts, and notifications.

Clients and vendors typically see over 50% improved efficiency via deep automation and customizability that streamline and simplify their workflows.

Furthermore, our clients can take their third-party risk management program to the next level with enhanced third-party risk assessment insights, actionable intelligence, and analytics that empower stakeholder and senior management business decisions.

Ready to learn more?
Book a free demo of Vendor360 today.

CENTRL

VENDOR RISK MANAGEMENT

Learn More: oncentrl.com/vendor360

Get a 1:1 Demo: oncentrl.com/demo-request

US/Global: +1 (415) 780-9667

UK/Europe: +44 020 3037 8609

Australia/APAC: +61 (02) 4910 3822

vendor360@oncentrl.com

/company/centrl

@oncentrl

More Resources

Enjoy this guide?

Visit https://oncentrl.com/resources for more best practice guides, blogs, and ebooks on global bank network management.

CENTRL

VENDOR RISK MANAGEMENT

CENTRL is a leading risk and compliance technology company that provides the most advanced software platform for managing third-party risk and due diligence. CENTRL offers solutions for automating vendor risk management, modern slavery act compliance, operational due diligence, and bank network management. CENTRL's platform is used by leading companies in all sectors across the globe.

US/Global +1 (415) 780-9667 | **UK/Europe** +44 020 3037 8609 | **Australia:** +61 (02) 4910 3822

And, for more information, please visit: oncentrl.com/vendor360

@oncentrl | /company/centrl/

Rev. 2022.01