VENDOR RISK

Find It Before It Finds You

Practical Guidance for:

- Identifying Risk in Vendor Relationships
- Defining Policies and Procedures to Manage It
- Finding Risk in the Vendor Selection Process
- Monitoring Vendors Over Time

An E-Book Presented By: Onspring RFP365

BEFORE YOU SIGN

Every business is a web of relationships between employees, clients and third parties. We rely on outside providers of products and services to help us achieve our strategic objectives, deliver value to our customers and empower our teams to succeed. This is true for organizations of all sizes, from the fledgling startup to the global enterprise.

Where we have vendor relationships, we also have risk. We may have well-defined, thoroughly tested controls within our own walls to reduce risk to tolerable levels, but we have much less visibility and authority over our vendors' environments. Holding our vendors to high standards for physical and cyber security, personnel management, and regulatory compliance is a challenge that can (and probably should) keep us up at night.

The truth is, we can't eliminate vendor risk unless we eliminate our vendor relationships. But we can take steps to identify and manage risk to levels we can accept. This e-book provides some practical advice for accomplishing just that.

The guide is divided into four parts:

1. Identify Sources of Vendor Risk
Understand a range of factors you should consider when evaluating vendors and the risks they pose to your organization.

2. Define Policies & Procedures to Manage It
Document your process for evaluating, selecting and monitoring vendors. Ensure that relationship owners know their responsibilities.

3. Find Risk in the Vendor Selection Process
Build vendor risk evaluation into your RFPs. Perform assessments and due diligence, and identify red flags in the contract review process.

4. Monitor Vendors Over Time
Carefully onboard new vendors and monitor their performance and adherence to your requirements throughout the relationship.

Whether you're just getting started with vendor risk management or you're building additional structure and rigor into your program, we hope you find this e-book to be a useful resource.

IDENTIFY VENDOR RISK

There's more to vendor risk than data breaches and fraud, though these two headline-grabbing issues are certainly top of mind.

It's also essential to consider more subtle forms of vendor risk. Remember, an issue with a vendor may not cripple your operations, but it could have deep and lasting impact on your brand and customer goodwill.

As you consider risks to your business stemming from third-parties, catalog those risks and make them accessible to your leadership team and to individuals who are responsible for vendor relationships. Creating **visibility** and **understanding** is the first crucial step to managing vendor risk across your organization.

When identifying sources of vendor risk, ask these questions:

- ❑ **Access to Sensitive Information:** Will the vendor handle your client or employee data, financial statements, intellectual property or other confidential information?
- ❑ **Operational Impact:** Would a disruption to the vendor's products or services harm your ability to carry out your own operations?
- ❑ **Revenue Impact:** Would a disruption to the vendor's products or services significantly impact your ability to generate revenue?
- ❑ **Reputational Impact:** Could misdeeds, negligence or malpractice on the part of the vendor damage your organization's reputation? (Think in terms of your clients, employees and the public at large.)
- ❑ **Resource Impact:** In the event of a disruption or issue with the vendor, how significantly would your internal resources be impacted?
- ❑ **Regulatory Impact:** Does the vendor relationship expose you to additional regulatory requirements (HIPAA, PCI, GDPR, etc.)? Would a disruption to the vendor's products or services impair your ability to demonstrate regulatory compliance?
- ❑ **Personnel Practices:** Does the vendor conduct background checks and policy training and awareness? What are the vendor's termination practices?
- ❑ **4th Party Risk:** How well does the vendor manage ***its own*** vendor relationships? What policies and procedures does the vendor have in place to ensure that you're not exposed to excessive 4th party risk?

DEFINE VENDOR POLICIES & PROCEDURES

Understanding the array of risks that vendors pose to your operations, strategic objectives and reputation is a crucial first step. But just as important: Defining how you will manage those risks and sharing this information with all employees.

This is where formal policies and procedures come into play. Document your process for evaluating, selecting and monitoring vendors, and ensure that relationship owners understand their responsibilities.

As with all policies, it's wise to track employee awareness and acceptance. Also, be sure that your vendor policy is accessible to employees at all times. When questions arise, "Consult the policy!"

When crafting your vendor management policies and procedures, consider these ideas:

- ❑ **Policy Scope:** Your policy should define requirements for third parties in the following areas (at minimum):
  - Human resources security
  - Physical and environmental security
  - Network and system security
  - Data security
  - Access control
  - IT acquisition and maintenance
  - Vendor management
  - Incident management
  - Business continuity / disaster recovery
  - Compliance

- ❑ **Risk Scoring Criteria:** If you're going to assess vendor risk, it's crucial to define your scoring methodology within your policy and communicate it to all vendor relationship owners. Organizations commonly separate vendors into three risk tiers: high, medium and low. There is no standard definition for these risk tiers, but when determining what's right for your organization, keep these factors in mind:
  - Criticality of the vendor's services in delivering your ***own*** products and services
  - Access to personally identifiable information (PII) for employees or customers
  - Access to non-public information (financials, strategic plans, intellectual property, etc.)
  - Level of spend and length of engagement
  - Any personal relationships between your organization and the vendor that may warrant a higher level of diligence

- ❑ **Procedures and Process Flows:** In addition to your vendor policy, employees will benefit from step-by-step guidance on ***how*** they should manage vendor relationships. Consider all parties that need to be involved: relationship owners, executive sponsors, legal, compliance, procurement, IT and other functions, along with the vendor itself.

  If your procedures are complex, a visual process flow can help people understand where they fit into the process and who is responsible for completing various tasks.

FIND RISK WITH SMART RFPs

If your vendor selection involves a Request for Proposal (RFP), it's a great opportunity to identify vendor risk early in the process.

As an RFP issuer, it may be tempting to focus on product functionality or service capabilities, leaving risk-related questions for downstream assessments. This may expedite your RFP, but it can create problems if your chosen vendor pushes you beyond your risk tolerance.

You can save yourself a few headaches by considering risk from the get-go. Bake risk evaluation into your RFP, and you'll be one step ahead when the time comes to closely assess your chosen vendor.

When issuing RFPs and evaluating responses, consider the following:

- ❑ **Requirements and Scope:** Be sure to gather requirements not only from the project team, but also from legal, procurement, IT, security and compliance. You may not include all of these requirements in your RFP, but you'll understand the full picture and can determine when and how to present certain requirements to potential vendors.

- ❑ **Deal Breakers:** Remember, it's not only your stamp of approval that matters. If you can weed out unacceptable vendors in the RFP process, you'll save yourself (and your extended team) a great deal of time in due diligence.

  When gathering requirements, be sure you understand the must-haves, nice-to-haves and deal breakers. Examples of potential deal breakers include (but are not limited to):

  - Critical audit findings
  - Failure to meet security standards
  - Lack of defined policies or procedures
  - Inability to meet budget or timeline requirements
  - Use of sub-contractors
  - Customer support concerns (outsourced, language barrier, etc.)
  - Lack of referenceable clients
  - Custom development required

- ❑ **Scoring:** Not all requirements are created equal, and high-dollar RFPs are especially delicate. The more money involved, the more stakeholders you need to satisfy and the more you need to factor risk into the evaluation process.

  Rather than considering each respondent separately and expressing their value qualitatively, develop a way to assign each respondent a numerical score. You can score by section (for example, functional requirements, security requirements, compliance requirements, etc.) or by individual question.

  Quantitative RFP scoring can help you:

  - Compare responses objectively
  - Focus on priorities
  - Justify selection criteria
  - More easily identify red flags

FIND RISK WITH DUE DILIGENCE

The due diligence process is the most obvious place to identify risk in vendor relationships. But how much time and effort should you spend on this? How much is too much? The answer is (annoyingly), "it depends."

The level of scrutiny you should apply depends on the nature of the vendor relationship. Vendors that have access to confidential data or who deliver business-critical products or services require a high degree of scrutiny. The effort is worth the investment.

But keep in mind that seemingly harmless vendors can expose your organization to risk. (Remember the HVAC vendor involved in the Target data breach?) It's crucial to apply a baseline level of diligence to all vendors, ramping up efforts for third-parties that expose your organization to greater levels of risk.

And in all cases, be sure to perform your due diligence ***before*** you sign a vendor contract.

When assessing vendors, try these strategies:

- ❑ **External Questionnaires:** Vendors that want to do business with you should be prepared to supply information about their business processes, control environment, insurance coverage, security certificates, client references and any pending legal action. If they're reluctant to do so, take that as a warning sign.

  Once you've selected a vendor that meets your requirements, send them a questionnaire that they must complete in a timely manner. Your questionnaire can be a simple Excel spreadsheet, or you can use web-based software to securely collect information and documents, score responses, and house them in a central repository.

  If you don't have your own vendor questionnaire, you can use a product like the Standard Information Gathering (SIG or SIG Lite) questionnaire, issued by the Shared Assessments Program.

- ❑ **Internal Questionnaires:** It's also a good idea to ask relationship owners within your organization to evaluate new vendors. These questionnaires don't need to be burdensome, but they should cover some basic areas:

  - Relevant experience
  - Ability to execute
  - Reputation
  - Security and privacy
  - Compliance and controls
  - Impact to internal resources

  You want to be sure that the information you receive from the vendor aligns with the relationship owner's expectations. If you see a mismatch, dig deeper.

- ❑ **Expert Review:** Once you've collected information from vendors and relationship owners, it's important to get the "right eyeballs" on it. The review process is probably not a job for a single person. You may need to route information to legal, compliance, information security or IT for their expertise.

FIND RISK WITH CONTRACT REVIEW

By the time you reach the contract review stage with a vendor, it can feel like the point of no return. You've gone through the selection and assessment process, and the relationship owner and vendor are eager to push the agreement across the finish line.

But before you sign, carefully review all documents for red flags. These documents may include:

- Nondisclosure agreements
- Master license agreements
- Master service agreements
- Statements of work
- Quotes and order forms
- General contracts

A formal contract review process with a central information repository is helpful here. Your legal team will undoubtedly have questions for the relationship owner and the vendor, so equipping contract reviewers with instant access to documents, contact details and other metadata can save time and reduce the back-and-forth.

In the contract review process, ask the following questions:

- ❑ **Contract Duration:** How long is your agreement? What are your options for termination if the vendor fails to fulfill its obligations? Under what conditions can the vendor sever its agreement with you? What happens after termination?

- ❑ **Contract Value:** What is the total cost of the agreement, and what are the payment terms? How is your organization protected from overages? (Think in terms of data storage, services hours, user licenses, equipment failure, etc.) Does the value of the contract warrant another layer of review with executive management?

- ❑ **Performance Tracking:** How will the vendor prove that it is meeting its obligations? Are there defined milestones? Will you receive status updates or other documentation of completed work? By what measures will you hold the vendor accountable?

- ❑ **Special Clauses:** Does the agreement include any special clauses for termination, damages, indemnity, exclusivity, etc. that conflict with your internal standards? If yes, is the vendor willing to budge on these issues?

- ❑ **Warranty Restrictions:** Under what circumstances would any warranties for products or services be void? Are these stipulations reasonable and acceptable to your organization?

MONITOR VENDOR RELATIONSHIPS

The ink on the contract is dry and your vendor relationship has begun. At this point, you've gathered enough information to be reasonably confident that the vendor fits within your risk appetite.

You're ready to get down to business, but don't take your foot off the gas when it comes to risk evaluation and monitoring. This is no time to say, "we've checked all the boxes" and move on. To manage vendor risk effectively, you need to monitor performance and adherence to your standards throughout the relationship.

Unfortunately, this is no easy feat. You have limited visibility and authority over your vendors, so you must take steps to keep the lines of communication open.

Just remember: The onus is on the vendor to supply information and keep you informed. Your job is to communicate your expectations and enforce them.

When it comes to monitoring vendors, consider the following:

- ❑ **Onboarding:** Depending on the nature of the vendor relationship, you may need a formal onboarding process. During this time, you should ensure that the vendor profile is complete (contacts, deliverables, timelines, NDAs, W-9s, insurance certificates, etc.). Also, you'll want to carefully track which data or systems the vendor can access and for what reasons.

- ❑ **Resolution of Findings:** If you identified issues during vendor evaluation that remain open after the contract is executed, be sure to stay on top of those contingent items. It's easy to lose track of findings once the vendor relationship is underway. To prevent this, require regular updates from the vendor until all issues are resolved to your satisfaction.

- ❑ **Status Reports:** Also require the vendor to provide regular updates on the status of the project or engagement. This doesn't need to be overly burdensome, but the vendor should keep you updated on work completed, progress toward milestones and any project risks.

- ❑ **Onsite Audits:** It may be necessary to go onsite with a vendor to monitor their adherence to your standards. For example, do their employees follow the clean desk / clear screen policy? Do they have adequate controls on physical access points and surveillance equipment? Under certain circumstances, you may need to "see it to believe it."

- ❑ **Satisfaction Surveys:** On an annual basis (and certainly before you renew a contract with a vendor), survey the relationship owner and other impacted parties to determine whether the vendor has fulfilled its obligations and met your organization's needs. You'll be surprised how often you find that your internal stakeholders do not like a vendor! In these cases, why continue the relationship? Small problems that annoy your team could be a warning sign of bigger issues.

FINAL THOUGHTS: THE ROLE OF TECH

Though we may try to boil vendor risk management down to its most basic concepts, the fact remains that it's a complex process, involving a number of business functions and often large volumes of data. It's difficult to get a handle on all the moving pieces without the benefit of technology.

Spreadsheets, email and shared drives can take you only so far. If you're dealing with a handful of vendors, these tools will probably suffice, but as your vendor relationships expand (by type, geography and complexity), you may find yourself in need to greater visibility, efficiency and control.

There's no single technology that will facilitate all aspects of vendor risk management for your organization. However, cloud-based platforms like Onspring and RFP365 can handle much of the heavy lifting. These products allow you to:

- Issue RFPs through a secure online portal
- Score responses and manage the evaluation and selection process
- Collect information and documentation from vendors through external surveys
- Perform and score vendor risk assessments
- Manage vendor profiles and track outstanding tasks or issues
- Facilitate the contract review process with automated workflow
- Find the information and documents you need at a moment's notice
- Report on vendors by status, risk rating, criticality, usage, spend and other criteria

ABOUT THE AUTHORS

Thanks for allowing us to share our insights and recommendations through this e-book. We hope you find the content useful as you implement or enhance your own vendor risk management program. Our recommendations are by no means exhaustive, but they provide a solid framework for understanding the sources of vendor risk and managing it in ways that make sense for your organization.

Questions? We're happy to help. Please find our contact details below.

Chris Pantaenius, Onspring

Chris is CEO of Onspring Technologies. He co-founded the company in 2010 to help business people solve complex problems through modern, flexible technology. As a career consultant and solution developer, Chris has deep experience in the areas of vendor and contract management, risk assessment, compliance, and business operations.

Connect with Chris: linkedin.com/in/cpantaenius
Visit our website: onspring.com

David Hulsen, RFP365

David is co-founder and business director of RFP365. He's responsible for sales and marketing, client services and financial operations. David has a long history of issuing and responding to RFPs as a technology consultant. He's passionate about using technology to bridge the digital divide, both across poverty lines and through improved corporate efficiencies.

Connect with David: linkedin.com/in/davidhulsen
Visit our website: rfp365.com