EMERGING TRENDS AND BEST PRACTICES IN VENDOR MANAGEMENT PROGRAMS

Vendor Centric

Emerging Trends and Best Practices in Vendor Management Programs

Published by Vendor Centric
9841 Washingtonian Boulevard, Suite 200, Gaithersburg, Maryland 20878

Visit us at www.vendorcentric.com.

CONTENTS

INTRODUCTION

In March 2018, more than 150 compliance, risk and vendor management professionals got together in Atlanta, Georgia for the 3rd Annual Third Party Risk Management & Oversight Summit.

Speakers and panelists included some of the leading thinkers and practitioners in vendor management today from organizations like:

- **Abercrombie & Fitch**
- **Bank of America**
- **Fidelity Investments**
- **Henry Ford Health System**
- **National Basketball Association**
- **Target**
- **The Coca Cola Company**
- **Under Armour**

We were excited to participate in a conference dedicated to the emerging business discipline of vendor management, and to hear from other experts in the field. There is a growing consensus that vendor management continues to transition out of the compliance department and into a core business discipline that must be practiced across the enterprise.

With so many great insights and ideas shared at this conference, we decided to bundle-up some of the highlights and share them with you.

Enjoy!

THESE VENDOR RISKS ARE KEEPING SENIOR EXECUTIVES UP AT NIGHT

THESE VENDOR RISKS ARE KEEPING SENIOR EXECUTIVES UP AT NIGHT

Businesses in the financial services, healthcare and nonprofit sectors are heavily regulated with regard to procurement, contracting and management of relationships with third party vendors. Complying with those regulations is critical. However, the days of vendor management being purely a 'compliance' issue are fading away. More and more organizations are elevating the conversation about vendor management from a focus on compliance to, instead, a focus on risk.

In a session titled **Think Tank: What Keeps You Up at Night**, risk, compliance and vendor management professionals from Abercrombie & Fitch, Centene Corporation and Ionic Security shared their thoughts on some of the ongoing and emerging vendor risks that keep them up at night.

Pay attention - you may just recognize some of these in your own organization.

Data Management and Security Risk

In 2017, more cybersecurity breaches were reported than in any other previous year. The panelists agreed these breaches are only going to grow in frequency and impact. Knowing which of your vendors are collecting and storing data, and focusing heavily on monitoring and managing the data and security risks with these vendors, should be a major priority for everyone.

Operational Risk

As reliance on vendors for critical business functions continues to increase, so does the risk those vendors pose to business operations. Mitigating these risks requires an understanding of your vendors' own processes and operations, and insight into their health to ensure they can not only provide the level of performance that's expected, but that they'll be there for the long haul.

Regulatory Compliance Risk

CMS, OMB and OCC are only a few of the regulatory bodies targeting better management of third party vendors. Panelists agreed this is only the start, and regulatory compliance requirements for vendor management will continue to expand. It's critical that compliance be part of, but not all of, your vendor management program.

Geographic Risk

Abercrombie and Fitch sources goods from all over the world, and has identified 20 countries with a high risk profile. When they work with vendors in these countries, they perform additional due diligence in the initial risk assessment process. They extend these activities into their post-contract oversight and management too.

5. Downstream Vendor Risk

An emerging area of vendor risk management is downstream vendors. For example, Centente Corporation (healthcare) outsources a significant amount of work required to deliver care to their insured members. This not only means they place a heavy reliance on their direct vendors, but also the ability of their vendors' vendors (i.e. downstream vendors) to also deliver. Gaining visibility into these downstream vendors, and ensuring they are being risk assessed (and managed), is critical to ensuring consistency of quality care.

> "Knowing which of your vendors are collecting and storing data, and focusing heavily on monitoring and managing the data and security risks with these vendors, should be a major priority for everyone."

6. Reputational Risk

While not a risk on its own, everyone agreed that their own organization's reputation is one of their biggest concerns when it comes to vendors. Third party data breaches like the ones that happened at Walmart, Equifax and Goodwill are great examples. When consumers share information with companies, they expect those companies to protect it. And that includes monitoring their vendors as a normal course of business. When this doesn't happen, many consumers are simply packing up and leaving. No business can afford that.

Do any of these risks hit home with you? If so, now's the time to evaluate your own vendor management program to ensure you're able to identify and mitigate these risks before problems arise - if they haven't already.

FOUR STEPS TO CONDUCTING AN IMPACTFUL VENDOR RISK ASSESSMENT

FOUR STEPS TO CONDUCTING AN IMPACTFUL VENDOR RISK ASSESSMENT

As vendors become more intertwined in day-to-day operations, vendor risk assessments are growing in adoption. Doing a proper risk assessment allows you to understand the level of risk you assume in each vendor relationship, and make informed decisions about how to mitigate and manage those risks. Or in some cases, avoid an unnecessarily risky vendor relationship before it's too late.

In a session titled **Conducting Risk Assessments for Various Third Parties**, panelists shared a four-step process for conducting vendor risk assessments that can scale to companies of different sizes and industries.

1. Develop Vendor Risk Criteria

Before you can do a risk assessment, you must first define the criteria on which you want to evaluate risk. There are lots of potential criteria to consider, and many industries have vendor risks that are important to them. For example, vendors who collect or store personal health information (PHI) present a very high risk in the healthcare industry. So it's important that you view your risk criteria through your own, unique lens.

With that said, there are several vendor risks that are common across many industries.

- **Operational Risk.** How important is the vendor's work to your organization's business activities and operations?
- **Data/Privacy Risk.** Will the vendor be collecting or storing any data on your customers, members, donors or employees?
- **Transactional Risk.** Will the vendor be processing any of your financial transactions?
- **Replacement Risk.** If the vendor were to go out of business due to financial insolvency or other issues, could you replace them quickly to avoid disruption to operations?
- **Downstream Risk.** Will the vendor be using their own vendors (i.e. fourth and fifth parties) who play a role in the delivery of your products or services?
- **Compliance Risk.** Are there vendor-related regulatory issues with which you must comply?
- **Geographic Risk.** Is the vendor located in a region or country in which it is inherently risky to do business?

2. Create a Preliminary Vendor Risk Profile

Once your risk criteria are identified, you will use them as the basis for a formalized risk assessment. In your assessment you should evaluate the risks of a new vendor relationship based on your risk criteria, and establish a preliminary risk profile of the vendor. This allows you to understand where your inherent risks lie with the vendor, and assign an appropriate level of due diligence.

When doing this, most companies create different tiers for their risk profiles. The most common are high, medium and low tiers of risk, but the number of tiers is up to you. The higher the risk tier, the more due diligence you will need to perform to evaluate each of the risks and how well they can be mitigated and managed.

3. Perform Due Diligence Based on Risk Profile

Once the risk profile is established, the next step is to perform vendor due diligence to assess the risks you've identified. The riskier vendors will require more up front due diligence and, if you end up contracting with them, a higher level of ongoing oversight too.

Good vendor due diligence allows you to collect the right (and right amount) of information based on the vendor's risk profile. Most companies collect information through the use of due diligence questionnaires, and supplement those with other documents such as audited financials, SOC 2 reports and disaster recovery plans.

Once the information is collected, you'll need the right subject matter experts to help analyze it. This may require involving IT, security, finance, compliance or other experts to evaluate responses and reports. Some organizations also establish committees to help manage this process.

There are unique challenges to performing vendor due diligence when working with smaller companies; especially those that are privately held. Many won't have audited financials or SOC 2 reports, so you'll need to be flexible in how you assess those areas.

On the flip side, larger vendors may have an abundance of information but may require a more expansive due diligence process. This can include triangulating their responses with information from other data services (like Dun & Bradstreet Supplier Risk Manager). They may also require you to perform on-site visits to walk through and test processes.

Just remember that you don't need to apply the same level of due diligence to every vendor. Align your activities with your vendor risk profiles to be both efficient and effective in this process.

> "Know that the goal of the vendor risk assessment process is not to eliminate all risks, but to use real data to understand what those risks are and determine how you're going to mitigate and manage them."

4. Address the Risks You've Uncovered

The final step in the process is to actually take what you've learned and determine what to do with the information you've collected. Does the vendor have adequate systems and controls in place to mitigate the identified risks? Are there additional steps you need to take to further evaluate processes? Or is there simply too much risk to do business with that vendor?

Know that the goal of the vendor risk assessment process is not to eliminate all risks, but to use real data to understand what those risks are and determine how you're going to mitigate and manage them.

Two of the most common ways to manage vendor risk are through well-designed contracts and ongoing vendor oversight activities. So it's important to coordinate with legal during contracting, and the actual business units post-contract to ensure there is an appropriate level of ongoing vendor management.

The reality is that the "problem" of vendor risk isn't going away. Business relationships are becoming more complex, and vendor risk assessments have transitioned from a 'nice-to-have' to a 'requirement'.

Make sure you have a good process in place to know who your riskiest vendors are, and proactively manage those risks throughout the lifecycle of the vendor relationship.

FIVE PRIORITIES FOR TARGET'S VENDOR MANAGEMENT PROGRAM

FIVE PRIORITIES FOR TARGET'S VENDOR MANAGEMENT PROGRAM

Target did nearly $70B in revenue in 2016 and worked with vendors in more than 50 countries. So it's hard to believe that the retail giant only started their third party risk management program (TPRM) in 2015! But that's exactly what we learned in a session titled **Assessing the Financial Viability of Third Parties to Maintain Compliance and Operational Resilience.**

Sarah Fercho, Director of Vendor Risk Management at Target, noted that shortly after the program was formalized it was determined that the best place to focus initially would be with Target's highest risk vendors in both merchandising and non-merchandising. So in 2016, Sarah and her team risk rated their vendor relationships, identified those that were most important to Target's operations and business continuity and begin executing their TPRM activities.

As they rolled things out, they developed a set of five priorities for vendor management that served as the focal point for their efforts. They were simple yet substantive, and provided guidance on where to focus efforts across their portfolio of thousands of vendors.

1. Knowing with whom Target does business

Target collects important information about all aspects of the vendor relationship and stores everything in a central system. This provides transparency to all of the TPRM stakeholders.

2. Protecting Target's interests with appropriate contracts/agreements

Contractual standards and templates are used, and roles and responsibilities for contract development, approval and authorization are clearly defined.

3. Conducting consistent onboarding

This allows the vendor management team to set expectations and make sure every vendor knows how to do business with Target.

4. Monitoring the relationship throughout the vendor lifecycle

Target uses a coordinated approach to managing the vendor relationship from cradle to grave. This begins during the sourcing and procurement stages, and continues through contracting, onboarding and continuous performance management and risk assessments.

5. Executing intentional off-boarding

When vendor relationships end, they don't just dissolve into nothingness. They are transitioned in a thoughtful, deliberate way. This ensures an effective transfer of knowledge and data, and coordinated closure of all contractual responsibilities and terms that were agreed upon.

"Target uses a coordinated approach to managing the vendor relationship from cradle to grave."

The responsibility for adhering to these tenets doesn't live in one place – it permeates the entire company. There are actually three lines of defense which starts with the business units (first line), moves up through management and specialty departments like compliance and procurement (second line), and ultimately bubbles up to committees of the board of directors (third line). Also, the highest risk vendors require an Executive Sponsor (VP) and a day-to-day relationship manager.

The recency of the formalization of Target's third party risk management program is a reminder that the business discipline of vendor management is still emerging - even to a company with nearly $70B in annual revenue.

But evolving regulations for managing third parties, and a continued increase in cybersecurity breaches, is driving more formalized adoption of vendor management in organizations of all sizes.

SEVEN TIPS FOR A SUCCESSFUL VENDOR DUE DILIGENCE PROCESS

SEVEN TIPS FOR A SUCCESSFUL VENDOR DUE DILIGENCE PROCESS

Conducting effective vendor due diligence is as much art as science. It was a hot topic at the summit, as professionals from more than a dozen industries shared there tips and best practices for conducting effective vendor due diligence. Here are seven that we liked best.

1. Set the right tone at the top

Senior management (as well as the board) must buy into the fact that managing vendor risk is an enterprise-wide initiative and not something that 'comes from compliance'. This positions vendor due diligence as a required business practice, versus a nice to have, and allows for repercussions to occur if it's not handled properly.

> "Senior management (as well as the board) must buy into the fact that managing vendor risk is an enterprise-wide initiative and not something that 'comes from compliance'."

2. Consider a steering committee

Most organizations don't have a formal vendor management office, and many don't even have a central procurement department. Given the myriad stakeholders that can be involved in due diligence - procurement, compliance, risk, IT, finance and, of course, the actual business owner – a vendor management steering committee can be a way to provide governance to the due diligence process. This group can ensure the right questions are asked, and only properly vetted vendors come on board.

3. Communicate the value of vendor due diligence to your front line

The actual buyers of goods and services in your organization are most important to triggering the due diligence process. Help them understand that good due diligence will ultimately benefit them, not you.

4. Align due diligence activities with risk profiles

Not every vendor carries the same amount of risk, so due diligence should align with the risk profile of the vendor. Use a set of gating questions to initially tier your vendors based on what they do and the risks they bring. Then align your vendor due diligence activities based on those risk profiles – more risk equals more due diligence.

5. Build due diligence into the procurement process

Incorporate due diligence questions into the RFP/RFQ process with prospective vendors. This allows you to begin identifying potential risks and plan your due diligence activities early in the process.

6. Automate questionnaires and document collection

Using vendor management software to automate the due diligence process ensures consistency, provides visibility into compliance and drives the process much deeper into your organization.

7. Reassess vendors on a periodic basis

Due diligence is an ongoing activity and doesn't end at contracting. Best practices are to perform an appropriate level of due diligence throughout the lifecycle of the vendor relationship to ensure things haven't changed since your initial assessment.

A strong due diligence process is a must if you want to properly understand and mitigate vendor risk.

Conference attendees all agreed – don't skimp on the process, especially with your higher risk vendors. There are too many opportunities to regret it if you do.

NINE CONTRACT PROVISIONS THAT MITIGATE VENDOR RISK

NINE CONTRACT PROVISIONS THAT MITIGATE VENDOR RISK

Negotiating the right provisions in your contracts is one of the most important things you can do to mitigate and manage risks in your vendor relationships.

In a session titled **Mitigating Risks with Critical Contract Provisions and Termination Clauses**, vendor management professionals from Henry Ford Health System and Bank of America Merchant Services shared their insights on the contractual clauses that are most important to them.

1. Business Continuity and Disaster Recovery

Covers what happens in the event of a service interruption. Should include the right to test a vendor's business continuity plans.

2. Data Ownership and Transfer

Identifies who owns the data that is collected and/or stored, and the process to be followed in getting that data back when you want it.

3. Indemnity and Liability

Allows for relief in the event a vendor does something wrong or fails to perform, and sets the limits around losses incurred as a result of a vendor failure.

4. Information Security and Privacy

Different from data ownership, it restricts the use of the data by permitting the vendor to use data only as required to perform the services.

5. Right to Audit

Provides the ability for you to audit the vendor's operations and records to ensure they are meeting contractual requirements, industry standards and/or compliance with laws and regulations.

6. Scope of Services

Defines the nature of the services/products, timing, delivery methods and location. You'd be surprised how often these are too vague to hold anyone actually accountable.

7. Service Level Agreements

Establishes agreed upon expectations for service levels the vendor must meet. These are common in technology and outsourcing contracts, and should address expectations for non-performance or breach, and penalties for both.

"Incorporating the right provisions into your vendor contracts allows you to mitigate risk at the start of the relationship rather than "putting the toothpaste back in the tube" later on."

8. Subcontractor Relationships

Requires the identification of 4th parties the vendor may use, and how the vendor is going to monitor their compliance with applicable contractual agreements.

9. Termination Events

Defines what triggers termination, and the transition activities that must occur to affect an orderly transition.

Incorporating the right provisions into your contracts allows you to mitigate risk at the start of the relationship rather than trying to "put the toothpaste back in the tube" later on. It also allows you to balance the acceptance of risk and liability in your agreements that makes sense for both you and your vendors.

10 BEST PRACTICES FOR EMERGING VENDOR MANAGEMENT PROGRAMS

10 BEST PRACTICES FOR EMERGING VENDOR MANAGEMENT PROGRAMS

Vendor management is an emerging business discipline, being adopted with greater frequency by companies across a variety of industries. Part of this emergence has been a transition from a purely compliance-based function to an enterprise risk-management function, oftentimes residing outside of compliance in its own vendor management office.

But there is no one-size fits all when it comes to a vendor management program. Rather, size and complexity should scale to an appropriate level of maturity for every organization As you evaluate how to right-size a vendor management program for your organization, consider the best practices highlighted below.

1. Right size your vendor management program for you.

Many companies delay starting a vendor management program because it seems overwhelming. Our advice – don't try to boil the ocean. Figure out what matters most to you, and right size your program using a vendor management framework like the one we've developed at Vendor Centric.

2. Set the right tone at the top.

Your leadership must buy into the fact that vendor management is a core business discipline and not a compliance function. It's critical to have buy-in from senior management (and the Board, when applicable) for the program to have teeth, and deliver the type of measurable value it's capable of.

3. Establish governance and engage your stakeholders.

Vendor management involves multiple stakeholders and subject matter experts from across the organization. In addition to the Business Owner who actually manages the vendor relationship, you may need to coordinate with procurement, finance, legal, risk, compliance and IT. Whether it's a formal vendor management office or a vendor management committee, make sure you establish a governance structure to provide direction and ownership for the program.

4. Get visibility into your vendors and contracts.

Too many organizations lack even the basic systems to know who their vendors are and what contracts they have with them. Data and documents reside in multiple places including emails, shared folders and file cabinets. You can't run a vendor management program with incomplete and disparate data. You need a central system for storing, managing and reporting on vendor-related information.

5. Know which risks apply to which vendors.

Not all vendors are created equal, and different types of vendor relationships bring different types of risk. Vendor risk assessments and tiering are core components of your vendor management program. They allow you to know where your risks are with every vendor relationship, and align your due diligence activities accordingly.

6. Don't skimp on due diligence.

Assessing risks is only part of the process, though. Due diligence is where the rubber meets the road in terms of drilling down to really evaluate risk exposure in your vendor relationships. Be sure to align your activities with the risk level of the vendor – more risk always requires more due diligence.

> "You can't run a vendor management program with incomplete and disparate data. You need a central system for storing, managing and reporting on vendor-related information."

7. Be disciplined in contracting.

Contracts are your only opportunity to legally document the business terms to which you and your vendor have agreed. Yet contracting is an inconsistent process in many organizations, resulting in unclear expectations and unnecessary risk. Your vendor management program should provide for a standard, consistent contracting process that ensures all of the necessary, risk mitigating contractual clauses are incorporated into the final agreement.

8. Establish expectations during onboarding.

Vendor management doesn't stop once the contract is signed. Rather, that's when most of it begins. Your vendor management program must address what happens post-contract and who will be responsible.

9. Monitor and grow the relationship like you would any other.

Developing a strong, mutually beneficial relationship with your vendor requires an investment from both of you. It also requires following a consistent process for continually evaluating performance, costs, risks and compliance. This is where the relationship can blossom and provide tremendous value, or fall flat and lead to big problems. Nurture your vendor relationships to get the most value from them.

10. Have a formal process for breaking up.

When the relationship needs to end, don't guess on what to do next. Have a formal process for off-boarding your vendors, especially as it pertains to key contractual requirements such as transfer of assets, data, or destruction of confidential information. You don't want to leave this stuff to chance. So don't.

At Vendor Centric, we believe that a formal vendor management program is as necessary to a business's long term success as is a formal human resource (HR) program. After all, businesses invest their financial resources with both employees and vendors, so it's only logical that both need to be managed effectively if those investments are going to produce the desired results.

If you need a hand with your vendor management program, we're here to help.

info@vendorcentric.com

240-813-1170

www.vendorcentric.com

Vendor Centric specializes in helping organizations create and maintain disciplined policies, procedures and systems for vendor management. Our software and services enable our clients to mitigate risk, control costs, ensure compliance and drive higher levels of performance with their vendors.

WWW.VENDORCENTRIC.COM