Third Party Risk Management
Cost-effective Approach
By Nikolay Filipets
# Table of Contents

Abstract .................................................................................................................................. 3  
Introduction ........................................................................................................................... 3  
Background/Historical Analysis .............................................................................................. 3  
Third-party Risk Management Approach .............................................................................. 4  
Methodology ........................................................................................................................... 5  
   Engagement/Selection & On-boarding ................................................................................. 5  
      Identifying inherent risk and scoping in supplier for oversight practices ......................... 5  
   Defining required controls ................................................................................................... 6  
   Assessing supplier to identify real risk ............................................................................... 6  
   Defining risk treatments and managing issues .................................................................. 7  
   Risk rating of supplier ......................................................................................................... 7  
Business Management ........................................................................................................... 7  
   Defining key roles and responsibilities .............................................................................. 7  
   Managing the relationship and performance .................................................................. 7  
   Overseeing the Supplier ...................................................................................................... 8  
   Recognizing supplier ......................................................................................................... 8  
   Decommission ................................................................................................................... 8  
Future Considerations/Research Directions ........................................................................ 8  
Conclusion ............................................................................................................................. 9  
References ............................................................................................................................... 10
Abstract

This paper focuses on importance of third-party risk management and outsourcing risks. Specifically this paper will emphasize the importance of building supplier relationships in safe, secure and productive way applying risk-based approach to supplier oversight and relationship management. Benefits and challenges outlined along with recommendations on how to build risk averse and policy compliant corporate culture.


Introduction

Outsourcing and offshoring are two of the most popular topics that we hear about from leading business analysts, news channels, newspapers or politicians. While the topic is very controversial in terms local socio-economic needs, there are clear financial benefits in engaging third parties to perform work that may not be a core business expertise of the employing entity. Companies that employ a third party to perform job on their behalf delegate a lot of responsibility and usually decision making authority to a separate entity and with that, of course, comes a lot of responsibility and oversight. In this paper the author will describe best in class third party management practices and risk-based supplier oversight approach on the example of the St. Louis-based pharmacy benefit manager company – Express Scripts.

Background/Historical Analysis

Imagine yourself having a family where you have a newborn baby that needs 24/7 care and this is also a family where both parents have successful and promising careers in major corporations. Of course in majority of scenarios neither of parents would want to completely quit their job for undefined period of time, but instead they would look for a day care or for an in house babysitter. In other words they would find a third party who specializes in taking care of newborns – essentially they would outsource it. Lets say we decided to go with a baby sitter, lets think about how would we go about finding one. First, we would probably ask our good friends and/or posted an add in a good newspaper. Next we would come up with requirements for our baby sitter, experience, references, etc. Then we would probably spend time interviewing and negotiating salary, and upon hiring a babysitter we would be managing/checking how good of a job that person is doing, and if our new born is happy, clean, feed, etc. and finally when we no longer need a baby sitter for the baby we would probably stopped paying our babysitter, cancelled the service and asked to return any keys, books, or toys - pretty straightforward approach, right? So why don’t we apply the same method to the outsourcing and third party risk management?

What is a general thought when people talk about outsourcing or third party risk? A lot of times we would probably hear comments like: “Most of our jobs are going to India!” or “China produces everything for the US, and we need to manufacture our own products!” With the
amount of security breaches that happened in the past few years, more often we hear and think about outsourcing and third party risk in a completely different way. Outsourcing has become topic of reliability, quality, and risk rather than topic of political debate.

According to Deloitte’s Global outsourcing survey outsourcing market is expected to grow and expand the scope of products and services that are outsourced to a third parties for manufacture or supports. While use of third parties is nothing new – merchants and companies have been using vendors and outsourcing various activities for years, the business eco-system drastically changed even in the past 10-15 years. And with increasing regulatory guidelines organizations face ever growing demand for effective and cost-efficient practices to perform third party risk management and oversight.

Third-party Risk Management Approach

It is no secret that every profitable and successful company cares about its bottom line, because it is very important to stay as efficient as possible and cut down operational expenses. Consequently, often times it is very hard to justify an overhead expense that would be created by additional activity related to risk management activities and oversight of suppliers. In case with Express Scripts there were just two full time employees who initiated the process to centrally manage third-party risk in a cost efficient manner through Risk Based Supplier Management Program. This approach involved connecting a set of cross-functional teams and forming a centrally led program that would incorporate subject matter experts from different organizational areas to manage third-party risk exposure. Express Scripts took a risk based approach to third-party risk management to ensure that suppliers provide productive, safe services and products that do not expose the company to excessive risk and adhere to quality, security and compliance standards. This approach also enables the company to identify, access, prioritize, and manage supplier risk, while managing the associated client and regulatory requirements.

Risk Based Supplier Management Program (RBSM) includes multiple supplier oversight processes, which include supplier audits, compliance assessments, information security assessments, physical security assessments, quality monitoring, quality accreditation assessments, service level agreements monitoring, and periodic supplier relationship performance scoring. Control deficiencies discovered through these processes and governed by the RBSM program.
Methodology

The Risk Based Supplier Management Program governs risk associated with outsourcing and required third-party oversight. The RBSM Program utilizes expertise of internal RBSM stakeholders throughout the life cycle of supplier to ensure suppliers receive coordinated assessments and audits. Suppliers are scored into the program based on the nature of products and services provided. The third-party oversight processes are woven into the company’s operations strategy and carried out via the supplier life-cycle:

1. Engagement/Selection & On-boarding
2. Business Management
3. Decommission

RBSM Program Supplier Management Lifecycle

Engagement/Selection & On-boarding

Business Management

Decommission

Engagement/Selection & On-boarding

During the engagement/selection and on-boarding RBSM Program performs a thorough assessment of prospective suppliers and their services or products before executing contract. The supplier’s control environment is evaluated to access their ability to meet company’s quality, security and compliance standards. Key activities performed during this stage include the following:

- Identifying inherent risk and scoping in supplier for oversight practices
- Defining required controls
- Assessing supplier to identify real risk
● Defining risk treatments and managing issues
● Risk rating of supplier
● Advising on necessary contractual terms and conditions
● Ensuring risk assessment process occurs prior contract execution

Identifying inherent risk and scoping in supplier for oversight practices

New suppliers are screened that they are not on a governmental excluded Parties List, which would prohibit Express Scripts from doing business with them. Suppliers and nature of services or products are then being reviewed in detail with RBSM Program Stakeholders (refer to the list of stakeholders above) prior to executing contract. This thorough initial review of the pending engagement allows the RBSM Program to scope in the needed assessment procedures and oversight practices to ensure that the right oversight is applied at the right rigor at the right time to the right suppliers.

Defining required controls

Express Scripts mitigates risk through implementation of custom build controls based on the National Institute of Standards and Technology (NIST) 800-53. The RBSM program determines the supplier control framework required for the oversight of a given supplier and its products or services.

**RBSM Supplier Controls Framework**

- Access Control
- Physical & Environmental Protection
- Medicare Part D
- System & Communication Protection
- System & Information Integrity
- Personal Security
- Audit & Accounting
- Maintenance
- Awareness & Training
- Configuration Management
- Regulatory Controls
- Performance Monitoring

- BCP/DR
- Cloud Service
- Security Assessment & Authorization
- Privacy
- Identification & Authentication
- Incident Responce
- Media Protection
- System & Services Acquisition
- Fraud, Waste & Abuse
- Financial Stability
- InfoSys Documentation
- Quality Management
Assessing supplier to identify real risk

During this stage of the process suppliers are asked to complete an assessment questionnaire, provide policies and procedures documents, display evidence of effectively designed and executed controls and on as needed basis undergo a site visit. An assessment questionnaire usually consist of the following content:

- Compliance – will review all uses and disclosures of protected health information
- Information Risk Management – will review supplier information security controls
- Corporate Security and Safety - will review supplier physical security controls
- Business Resiliency Management – will review supplier business continuity and disaster recovery plans

The primary outputs of the assessment are listing of real risk or issues that need to be managed and remediated.

Defining risk treatments and managing issues

Risk treatments (or responses to identified issues) are required to be submitted by suppliers and involved internal stakeholders. Responses usually consist of actions to be taken and a timeline to remediate that risk.

In cases where supplier cannot comply and commit to remediation of risks, then specific delegated functions can be revoked, supplier may be assessed financial penalty, and/or the engagement with that supplier may be terminated.

Risk rating of supplier

The risk rating of each issue identified with a supplier serves as the basis to calculating the real risk of that supplier. These are aggregated to determine a risk rating and allow ranking suppliers’ relative risk that helps to identify and prioritize oversight requirements and frequency.

Business Management

Upon mutual agreement on terms and conditions of the contract and finalizing the signatures, supplier gets assigned supplier performance manager and business owner to manage day-to-day relationship with that supplier. Key activities performed during business management phase include:

- Defining key roles and responsibilities
- Managing the relationship and performance
- Managing change
- Managing Contract
- Overseeing the Supplier
- Defining risk treatments and managing issues
- Recognizing supplier
- Communicating service scope changes

**Defining key roles and responsibilities**

Role of supplier performance manager is to maximize the productivity, quality, and ensure compliance with standards and procedures, while business owners are usually senior level staff that owns relationship with supplier and authorized to make key decisions as it relates to a certain supplier relationship.

**Managing the relationship and performance**

Supplier performance managers continuously monitor performance through status meeting, supplier audits, and score carding.

**Key Performance Indicators (KPI)** are the measure of performance in various aspects of the supplier relationship; these include:

- **Technology** – Features and usability of the product or process that result in increased effectiveness.
- **Quality** – Adherence to agreed-upon standards of the product or process
- **Support/service** – The ability to support the product or services that increases company’s ability to serve its customers
- **Delivery** – Delivery or manufacturing of products or services within the expected delivery window
- **Business/management** – Compatibility of company operating cultures
- **Financial** – Value of services to the company
- **Compliance/environmental/safety** – A commitment to the health and safety of employees, the surrounding community and environment

**Overseeing the Supplier**

The RBSM program coordinates stakeholder oversight activities based on standard oversight practices, which include:

- **Assessments** – Assessing supplier to identify real risk
- **Attestations** – Medicare Part D suppliers are required to sign an annual attestation to confirm compliance with key requirements
- **Site Visits** – Performed periodically to ensure continued compliance and relationship building
- **Audits** – Suppliers audits performed periodically using risk-based approach.
• Service Level Agreements (SLA) – SLAs are the key strategic tool which ensures that outsourced business processes meet or exceed on-going needs and expectations
• Relationship Performance Score carding – Relationship status feedback provided on a regular cadence.

Recognizing supplier

Business owners nominate their suppliers for the supplier recognition program based on the status of the relationship performance scoring process, adherence to compliance requirements, and the ability to provide value-added service. Winners are determined by steering committee and recognized at an annual celebration and award ceremony.

Decommission

When the business no longer requires the service of a supplier the RBSM Program and stakeholders work to ensure that supplier decommission activities are conducted in accordance with the supplier’s contract. Decommission due diligence ensures that company’s data, intellectual property and assets are secured and/or destroyed at the conclusion of the contract.

Future Considerations/Research Directions

Based on the above overview it is very clear that the third party risk management takes a lot of resources, expertise and investment. Cross-functional program with risk based management approach employed by Express Scripts leverages experts from various departments and unites them to perform third-part risk management. According to KPMG’s research one of the top organizational risks in 2015 is third-party relationships and it is vital that third-party risk is precisely managed from multiple aspects and in a very detailed way. It is also important to maintain a cost-effective model to that would not increase overhead spend or introduce unnecessary expenses.

As third-party reliance increases is important to control oversight and management cost. Future consideration should continue for focus on providing complex oversight and risk management while managing the cost. To achieve this complex goal organizations should consider shifting oversight costs to the provider itself. For example in the Express Scripts’ case shifting supplier audit to be performed and paid for by the supplier would reduce cost to oversee for Express Scripts. Another approach to reduce the cost would be to create alliance of companies that would create an audit program that would meet objective of all companies in the alliance, and perform one time audit for supplier that is used by the alliance companies. In this case supplier would gain efficiencies as well and would not go through multiple audits and audit cost would be shared among the companies in alliance.
Conclusion

It is inevitable, that third-party support and reliance will continue to be one of the mechanisms to reduce cost and improve performance, however it is also important to note that under amplified regulatory requirements, current condition of digital markets and limited controls around cyber security, third-party risk management represents very complex business issue tight to company reputational risk and client/customer satisfaction.

Third-party risk management is a journey. Due to complex and changing market conditions, this area will always be evolving and adapting to new governmental regulations and security threats. However it is important to continue to optimize oversight practices and find the most efficient ways to engage in third-party relationships without over-exposing organization to unnecessary risks.

References


