An Integrated View of Supplier Risk

A whitepaper on the changing requirements of managing supplier risk

An Integrated View of Supplier Risk

Executive Summary

The role of suppliers has dramatically changed over the past fifteen to twenty years. Suppliers no longer simply provide core commodities or products, they perform a complex set of services that support the needs of internal customers for things like benefits administration, IT support, and facilities management. These suppliers also impact the satisfaction of external customers by providing core services like loan fulfillment, claims processing, and customer support.

While the potential reward from having core services delivered by third-party providers is significant, so are the risks. When asked about the sources of supplier risk, many people mention price fluctuation, supply disruption, and demand forecasts. These are all traditional and very real supply chain risks.

Today, the volatile economic climate, the amount of work being performed by suppliers, the increased regulatory environment, and the heightened concern about social responsibility and the environment require close scrutiny of the risk that can come from four other areas:

Viability – suppliers' ability to maintain a healthy operation
Performance – suppliers' quality of service to achieve expected value
Compliance – suppliers' discipline to adhere to internally and externally mandated guidelines
Social Responsibility – suppliers' alignment with internal social responsibility initiatives

When it comes to measuring these four areas, most companies treat each of these separately, if at all. Procurement and sourcing might assess the financial health of suppliers as part of the RFI process; departments and/or business units might set up KPI's to evaluate performance of outsourcing providers or the shared services center; and the operational risk group might define compliance requirements for key suppliers. This creates risk silos.

Another issue is that even when departments and business units define how these risk areas should be measured, they struggle to monitor each area in an on-going and consistent manner. Some groups use spreadsheets, others have created proprietary, point solutions, and some try to leverage their transactional procurement system to pull this information together.

An unfortunate outcome of managing risk in this manner not only is the increased exposure, but the added expense of third-party audits and a costly attestation process.

Therefore to manage risk effectively, organizations should have:

- Comprehensive programs that ensure an integrated view of supplier risk
- Consistent processes that ensure reliable assessments and evaluations

Comprehensive Programs

Vendor management and supplier risk have become an important topic for most companies. More and more, supplier risk is a topic of discussion among company directors and executives. Why? There are two main reasons:

1. A large percentage of core services is being performed by third party providers
2. A heightened regulatory environment holds companies accountable for their suppliers' actions

Together, these two trends demand that companies transition from simply monitoring supplier performance to implementing comprehensive risk management programs. Ideally, these programs should allow companies to measure and monitor the risk that comes from supplier viability, missed performance expectations, lack of compliance, and nonconformance with corporate social responsibility goals.

In addition, supplier risk programs should be managed in a well integrated manner, one that provides key stakeholders complete visibility into the risks that arise from lapses in viability, performance, compliance, and/or corporate social responsibility. While different functional areas may be responsible for collecting the data and evaluating the criteria that impact risk, all the information should be consolidated and accessible to all interested parties.

The goal of these programs is to stay ahead of potential problems and create an opportunity to work with suppliers to ensure that the value received equals initial expectations. The following four program types form the foundation of prudent supplier management.

Viability

As companies rely on third-party providers to deliver critical services, tracking the viability and health of key suppliers is imperative. Why? The risk of failure is very real. From 2007 to 2008, business bankruptcies increased 54%.[1] To reduce this type of supplier risk, companies should continuously monitor the following areas:

- Financial position – the financial health directly affects the ability of suppliers to perform their duties
- Legal actions/liens – the outcome of legal actions can have a profound impact on both the financial performance of an organization as well as its ability to deliver a good or service (e.g. breach of a patent) and liens are a good indicator of a supplier's ability to pay its bills
- Recent news – the news wires are excellent sources of information about a supplier. For example, the reduction of workforce, the award of a major contract, or the investigation by a regulatory body are all predictive indicators.

[1] Administrative Office of the Courts

Performance

It is hard enough managing the performance of internal tasks, let alone tasks being performed by third-party providers. What happens when service levels do not meet expectations? Internal and external customer satisfaction can be damaged, management costs can increase while attempting to bring performance back in line, and worse, revenue-generating services can be disrupted.

To help mitigate the risk associated with sub-optimal performance, companies need to identify key evaluation criteria, allow all stakeholders to rate performance, and have a way to communicate corrective action plans. To help avoid supplier risk associated with performance, programs should include the following attributes:

- Targeted KPI's and SLA's that reflect the type of relationship that a supplier has with the contracting company and the type of work being performed
- Clearly defined evaluation criteria that ensure consistency in how each stakeholder scores performance
- Active alerts and escalation to gain visibility into potential problems while they can still be corrected
- Flexible weighting based on both the item being evaluated and the person performing the evaluation to accurately calculate at risk fees

Compliance

When companies originally started outsourcing, there was a misconception that the responsibility for compliance was also being outsourced. Not so. The risk of not closely monitoring the compliance of suppliers can have severe consequences – from a loss in confidence by customers to fines levied by regulatory bodies.

In fact, in most instances, companies are as responsible for their suppliers' actions as they are for their own. For example, in the financial services industry, a key governing body, the Office of the Controller of the Currency, states the following:

> "A bank's use of third parties to achieve its strategic goals does not diminish the responsibility of the board of directors and management to ensure that the third-party activity is conducted in a safe and sound manner and in compliance with applicable laws."

And in the healthcare industry, the latest The American Recovery and Reinvestment Act of 2009, mandates that:

> "A business associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify the covered entity of such breach."

Unfortunately, most companies do not have a way to actively monitor the compliance of their third-party providers in areas such as:

- Financial – SOX, SEC, FCC, FTC, OCC Bulletin 2001-47
- Safety – OSHA, FDA, EMAS
- Data Privacy – HIPAA, GLBA, EU Data Protection Directive
- Security – IT, Physical
- Risk – Insurance, BCP, Political, Currency
- Legal – Patriot Act, Homeland Security, Conflict of Interest
- Quality – ISO, ANSI, CSA, ASME
- Trade – C-TPAT

A sound supplier compliance program must include:

1. A comprehensive understanding of the unique requirements of each supplier
2. A means to communicate these requirements and associated responsibility of each supplier
3. A framework to receive attestation from each supplier

Sustainability and Corporate Social Responsibility

Sustainability and corporate social responsibility have grown in importance during the past few years. For those companies that don't have programs in place, there is growing pressure to establish them. These programs cover broad requirements ranging from diversity, safety, and carbon footprint, to human rights and creating a positive impression on consumers.

For those companies that have programs in place, there is a growing trend to publically promote them.

So how can positive initiatives like these create risk for a company? One source of risk is created when suppliers don't act in accordance with the goals of these initiatives. And the risk is damage to the company's reputation.

A good example occurred when a major computer company announced that it had achieved its goals for becoming carbon neutral. Then the Wall Street Journal ran a story stating that the company's carbon footprint "doesn't include the oil used by its suppliers to make its computer parts, the diesel and jet fuel used to ship those computers around the world, or the coal-fired electricity used to run them."

Not the kind of press this company was expecting for all its efforts.

But the benefits from these programs are not simply good will – they have real macro and micro economic implications, and therefore, need to be monitored just as closely as a supplier's viability, performance, and compliance.

In today's environment, companies must communicate to their suppliers the specific requirements around sustainability and corporate social responsibility, so that each supplier understands its responsibility. Once these requirements are communicated, companies should closely track their suppliers against these established guidelines.

Consistent Process

As described above, the programs to track viability, performance, compliance, and sustainability and corporate social responsibility form the foundation of prudent supplier risk management. But to realize the full benefits, it is crucial that a consistent process be implemented to ensure the programs are fully leveraged. This process includes a number of important steps:

1. Segmenting suppliers into different risk categories
2. Determining the level of detail to monitor within each risk program
3. Measuring, monitoring, and communicating current status and necessary corrective action.

Segmenting Suppliers

Suppliers and service providers will present different levels of risk to a company depending on the type of work they perform for the company and the industry within which they operate.

The first step in building a supplier risk management program is to segment suppliers according to their risk profile (e.g. critical, high, medium, low). This segmentation can be based on many factors and will vary by industry. Some examples include:

- Amount of spend with the provider
- Level of direct contact with a company's customers
- Access to customers' personal information
- Strategic importance to company
- Operational impact

Ultimately, the segmentation will determine the level of scrutiny required for each supplier.

Determining the Level of Detail

As mentioned above, the segmentation will determine the level of scrutiny required for each supplier. For example, a supplier supporting a financial services company that is deemed to have a significant operational impact, has regular contact with company's customers, and access to personal data, will likely need to have a risk management program that closely tracks the suppliers' viability, monitors the suppliers' privacy program, and regularly checks the appropriate watch lists.

In selecting the level of detail to monitor, a balance between each program type is established. In some instances, considerable emphasis might be placed on the risk associated with non-compliance while in others each program type (i.e. viability, performance, compliance, and sustainability/CSR) might be weighted equally.

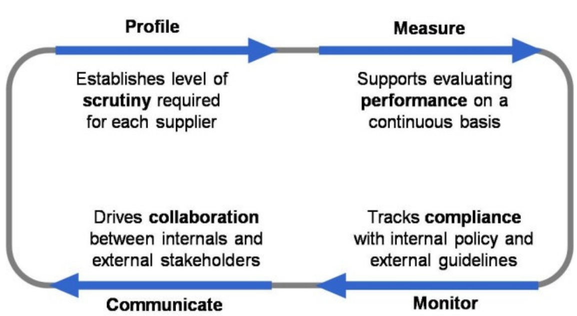
Regardless, it is important to note that there are potentially hundreds of criteria and requirements that could be used to monitor each area of risk. Therefore, it will be important to have access to a comprehensive library of the requirements for each program type. For example, what watch lists to monitor, what KPI's to use to measure performance for each function/activity being outsourced, what aspects of regulatory requirements should be monitored, and what sustainability and CSR guidelines should be followed.

Measuring, monitoring, and communicating

This last step is what ensures the success of supplier risk management. Without this step, despite all good intentions, overall risk will remain high. It is like putting together a plan for a big game and not playing it or choreographing a routine and not performing it.

Not surprisingly, this step is where many supplier risk management programs stumble. Successful supplier risk management demands a systematic, repeatable approach to:

1. Assign responsibility for providing input from internal and external stakeholders
2. Stay current about such things as a supplier's financial health, competitive threats, or legal issues
3. Track gaps between expectations and results and alert stakeholders so corrective action can be taken
4. Update reporting requirements as conditions and relationships change



Conclusion

Supplier risk cannot be outsourced. Companies must take responsibility for the overall actions of their suppliers whether because of internal guidelines, regulatory requirements, or public scrutiny. To effectively manage supplier risk, a holistic approach should be taken that segments suppliers into risk categories and then provides an integrated view across each supplier relationship.

This integrated view will pull information about the viability of the suppliers, their performance against set goals, their compliance with internal policy and external regulations, and their conformance with corporate social responsibility initiatives.

To gain this integrated view, a well documented and easy-to-follow process needs to be in place. Relying on each functional area and/or business unit to create its own process and tools is inefficient, costly, and cannot address today's broad set of requirements. There are hundreds, if not thousands of items to be tracked across wide geographies with many stakeholders.

Therefore, it is crucial to find a way that all key stakeholders – from internal users and service providers to board members and regulatory bodies, have the access and visibility to effectively manage the inherent risk that exists within a company's supply base and across its extended enterprise.

Mike Nolan, Global Head of Internal Audit, Risk & Compliance Services at KPMG, believes that "Ultimately, as risk and controls management becomes more strategic, more performance-related and more enterprise wide, it should form an increasingly important part of corporate DNA. It can rise to the challenge of becoming the fourth platform on which business is judged. Already institutional investors and rating agencies such as Moody's and Standard & Poor's are assessing organizations' appetite for risk and their capacity to control it, which helps to prove that there are competitive advantages to be had from efficient and effective risk and controls management methods and processes."

From these efficient and effective controls, an integrated and reliable view into risk is achieved and, in turn, produces tangible benefits:

- **Viability/Health**
  - Lower risk of operational failure
- **Performance**
  - Value Received = Expectations
- **Compliance**
  - Reduced exposure from noncompliance
- **Sustainability**
  - Decreased likelihood of reputational risk

Through collaboration with your suppliers, you will not simply be managing transactions and data, but delivering improvements in customer satisfaction, innovation, quality, and your company's reputation. In the end, a comprehensive supplier risk management program will have a profound impact on financial performance.

About Hiperos

Hiperos is setting the course for how companies manage their extended enterprise and manage the associated supplier risk. Our flagship product, R.Portal, is an on-demand service used to measure and monitor the performance, compliance, and sustainability goals of strategic providers. By combining rich functionality and a platform for peer-to-peer collaboration, Hiperos provides companies like TD Bank, Webster, and State Street with the capability to build collaborative supplier relationship management programs - programs intended to reduce costs, lower business risks, and drive improved company performance.

For more information, please visit our website – www.hiperos.com, or call our main office at (508) 460-7013

