Achieving Excellence in Supplier Risk Management

The 2008 financial crisis and its cascading effects have made it necessary to redefine the supplier risk management norms. The compliance responsibilities of suppliers have increased significantly over time.

Regulations have become broader, bringing suppliers under their purview along with the companies that utilize their services.[1] The changing regulatory landscape has further increased the scope of suppliers' oversight and replaced traditional methodologies and rules. The laws have always existed, but now suppliers will also have to follow these regulations.

With the increase in regulatory oversight, companies with limited knowledge and control over their suppliers may have to bear the brunt of the consequences for the misdeeds of their suppliers. These companies may face punitive implications, such as fines and penalties. The companies are now being called to raise the bar with regard to supplier oversight.

The current need is to have a robust supplier risk management framework that incorporates regulatory expectations.

Elements of Framework

A robust supplier risk management framework would typically include the following elements (**figure 1**).

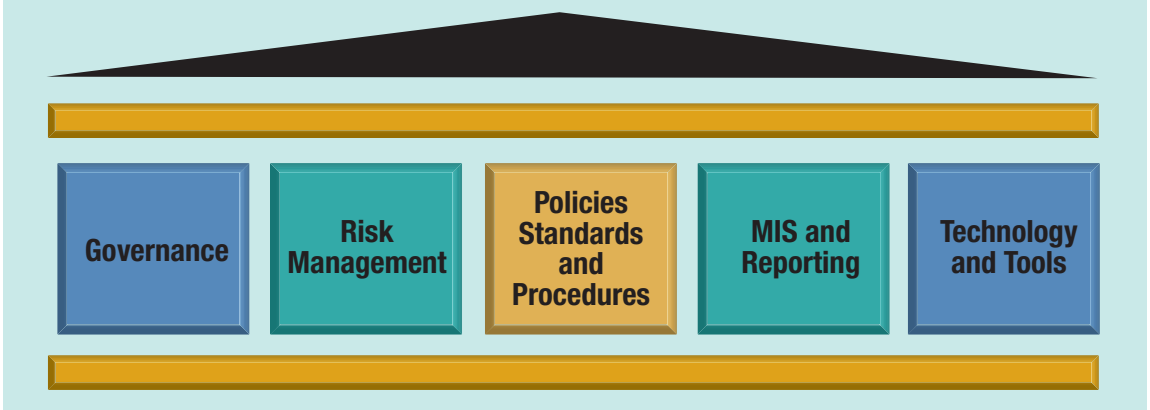
Governance
The role of governance is to establish clear roles, responsibilities and an escalation framework to manage risk pertaining to third parties across the supplier life cycle for a specific population of suppliers that are classified as more risky or critical than others.

This component requires developing a supplier oversight model and strategy that entails all risk management practices. The next step in the process is to determine the scope of suppliers, i.e., what should be in and what should be out of scope for monitoring and oversight purposes. There is also a need to define an owner within the organization to hold certain decision-making powers.

Risk Management
Management of supplier risk should occur through ongoing due diligence and oversight throughout the supplier life cycle. Risk management can be further subclassified as:

- Enterprise risk management, which entails managing risk at the enterprise level. The enterprise would be required to set an enterprise-level risk threshold based on the organization's risk appetite. Whenever the enterprise surpasses that threshold, response protocols will be initiated and must be implemented. In the worst cases, there

Figure 1—Elements of a Supplier Risk Management Framework



Source: Shirali Vyas. Reprinted with permission.

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® web site *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

Shirali Vyas, CA, ICAI
Is a risk consultant with risk management, process reengineering and project management experience. She provides consulting services to various financial services organizations on process reengineering and holistic risk management projects in the New York and New Jersey (USA) area.

would be a need to exit the relationship with the supplier.

In this component, enterprises are also responsible for:
- Drafting and implementing policies and procedures
- Implementing projects for enhancements to the various existing risk management practices
- Defining training requirements and awareness activities for the supplier population

- Business risk management, which involves activities such as contract compliance and performance monitoring, managing customer complaints, determining process criticality, and enforcing adherence to policies and standards by the suppliers

Policies, Standards and Procedures
A risk management methodology should be developed through well-defined policies, standards and procedures. They should be implemented through the ongoing monitoring of controls and compliance.

Management Information System (MIS) and Reporting
Reporting is required to increase transparency by providing a comprehensive view of supplier risk to all stakeholders across the organization, which, in turn, helps to identify, escalate, monitor and mitigate supplier-related risk and concerns and increase overall accountability.

Technology and Tools
To make these efforts successful, one must design and leverage a well-designed integrated system with work flow capabilities, which should be able to house all data under one system, enabling the tracking and monitoring of supplier data and issues on a real-time basis. This will help to provide the true picture of risk, which will enable the organization and risk managers to make informed decisions and identify and resolve issues in a timely manner.

Prerequisites for Success

The following will ensure a successful supplier risk management framework.

Define the total population of suppliers with which the organization has a relationship and tier the suppliers based on risk classification. As per the US Office of the Comptroller of the Currency (OCC), the definition of third parties includes all "entities that have entered into a business relationship with the firm."[2] In the *status quo,* organizations deal with tens of thousands of supplier relationships. Some reside in company records and some do not, e.g., those that are out of scope from the risk management perspective such as joint ventures, law firms, audit firms, complex relationships, fourth parties and co-branded partnerships, where the risk sharing is not defined. With the regulatory ambit growing to include all suppliers, having an up-to-date and comprehensive list of suppliers is the first step to start addressing regulators' concerns. Currently, many relationships are not subject to oversight, resulting in unknown and unaddressed risk, thereby increasing a firm's exposure.

Further classification of suppliers is required from a risk perspective or if the supplier is dependent on a particular vendor. Inherent and residual risk profiling

can help to identify and tier suppliers based on risk. Critical, complex and high-risk relationships must be monitored through the firm's supplier risk oversight framework and programs.

Identify all possible supplier risk, including emerging risk that can affect and expose the organization to financial losses, regulatory consequences and reputational damage. Given the changing regulatory landscape and emerging supplier risk, defining a comprehensive list of suppliers' risk to which the firm can be exposed by virtue of the relationship is a must for ensuring the success of a program. The risk factors identified should then be monitored by the lines of defense across the defined supplier population through various risk management practices, e.g., checking the supplier's reputation through news monitoring, event alerts and sanctions screening; monitoring the financial stability of suppliers through financial evaluations; and monitoring suppliers who may be sensitive to anti-bribery and anti-money laundering circumstances. In addition, the supplier risk list should be reviewed and proactively updated to accommodate emerging risk.

The Unified Compliance Framework's (UCF) approach is leveraged to identify all risk factors and map relevant controls to address risk. Risk assessments are designed to identify and address residual risk.

Use a risk-based approach when classifying suppliers. All suppliers cannot be treated the same. Classification of suppliers based on risk profiling and tiering helps to manage costs vs. benefits and efficiently allocate resources by conducting detailed due diligence activities for all high-risk relationships and limiting the scope of oversight for low-risk relationships. Existing risk management practices are augmented for suppliers. Suppliers who do not have access to confidential information do not need information security risk oversight; however, those suppliers should continue to be monitored for other risk to which they are exposed.

Create a robust, enterprisewide supplier risk management framework. The framework will be used to implement and monitor various supplier risk management practices. At an enterprise level, it should include defining enterprise principles, measures and thresholds. For each measure, thresholds should be identified and monitored across the supplier life cycle. Response protocols (accept, respond or continue to monitor) should be established to address threshold breaches.

Create an owner and escalation body for decision-making purposes. Creating a natural ownership model helps keep major decisions in a single group, which results in clear accountability and ownership. There may be instances when the level of exposure is so high that it cannot be managed exclusively by the business units or the first lines of defense. Such instances may require seeking guidance from, escalating to or requiring input from a higher body that has more decision-making authority. Business units should not be permitted to make these decisions in isolation without consulting the enterprise.

Supplier Risk Operating Committee

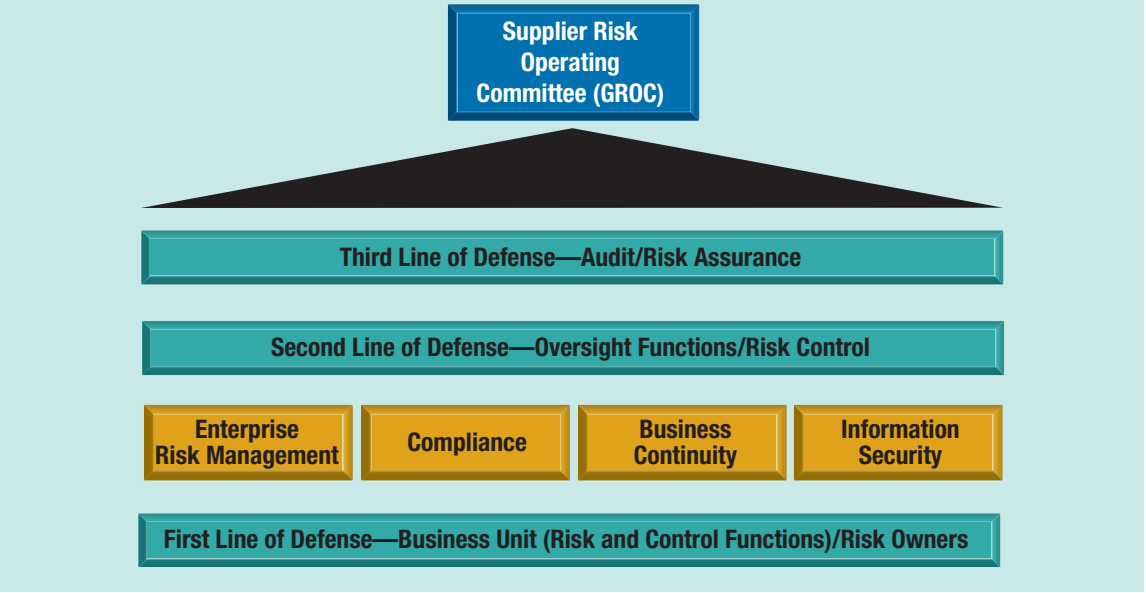
Assigning an owner with decision-making authority is essential for a governance and escalation framework. All three lines of defense, shown in **figure 2**, have specific roles and responsibilities defined in the supplier risk management framework.

It is the responsibility of the Supplier Risk Operating Committee (SROC) to maintain oversight and monitor the activities of the three lines of defenses and to ensure that a consistent approach is used across the enterprise.

Automated Technology and Tools

There is a lot of scattered information in various unconnected systems. For the framework to be effective, one integrated system that will provide the true overview on a real-time basis across the organization to different stakeholders, which will

Figure 2—Lines of Defense



Source: Shirali Vyas. Reprinted with permission.

allow risk managers to make informed decisions, needs to be developed. Data would flow from all stand-alone systems into the integrated system.

Governance, risk and compliance (GRC) solutions and risk convergence are leveraged to adopt an integrated risk management approach.

Implementation Plan

The framework for managing supplier risk at the enterprise level can be leveraged by sector, region and business as appropriate. First, one must determine activities and milestones that need to occur to implement the supplier risk management framework. Implementation activities include planning and design, education and promotion, program implementation, and GRC integration (**figure 3**).

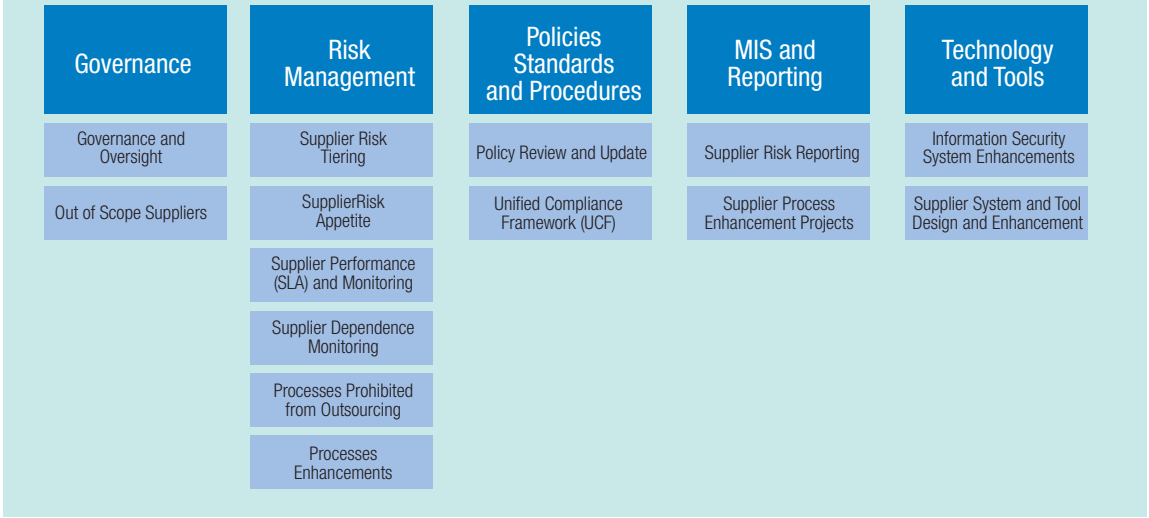
The supplier risk management framework provides a foundation, guidance, tools and technologies to manage third-party risk across the supplier life cycle. The framework also helps to ensure that the use of third-party suppliers, products and services does not result in business disruption. The framework is meant to assist organizations in managing and monitoring the risk exposure resulting from third-party suppliers and includes the following:

- **Supplier classification/supplier risk tiering**—High-risk suppliers can be defined as suppliers that provide critical products and services without which the company cannot operate effectively for even a short period of time. They could also have a revenue impact, regulatory impact or client dependency.

  Medium-risk suppliers include the category of suppliers that provides substantial products and services to the company and the supplier spend exceeds a certain limit. Supplier spend is the business volume managed by the supplier. The higher the managed business volume, the more critical or high risk the supplier is to the business. The volume can be defined by each business.

  Low-risk suppliers are those suppliers that are neither classified as high- or medium-risk suppliers. Alternatively, supplier tiering can be accomplished by performing risk assessments and arriving at the residual risk. The residual risk is equal to the control assessment rating minus the inherent risk.

Figure 3—Components of the Supplier Risk Management Framework



Source: Shirali Vyas. Reprinted with permission.

- **Supplier risk appetite**—Utilize industry best practice frameworks, such as the Committee of Sponsoring Organization (COSO) framework, to determine the supplier risk appetite and identify when a supplier relationship exposes the organization to excessive risk. Determine potential risk response protocols and risk tolerance levels that can be leveraged by the sector, region and business as appropriate. Invoke response protocols when the enterprise thresholds are breached.
- **Supplier risk reporting**—To enable enhanced oversight and increased transparency and enable real-time decision making, design supplier reporting and dashboards across different categories at supplier, supplier relationship, business, region and sector to show a high-level risk view and assessment rating.
- **Supplier performance (SLA) and monitoring**—Create a common set of key performance indicators (KPIs) and utilize them to measure and report supplier performance.
- **Supplier dependence monitoring**—Identify potential supplier relationships that pose concentration or dependence risk based on risk criteria or thresholds and measure and monitor risk. Supplier concentration or dependence risk is the probability of loss arising from heavily lopsided exposure to a particular group of suppliers.
- **Supplier process enhancement projects**—Design and implement process improvement projects to enhance processes and address gaps in process design, e.g., enhancements to the exit strategy process, supplier reporting, supplier onboarding, supplier system and records management.

Management Across the Supplier Risk Life Cycle

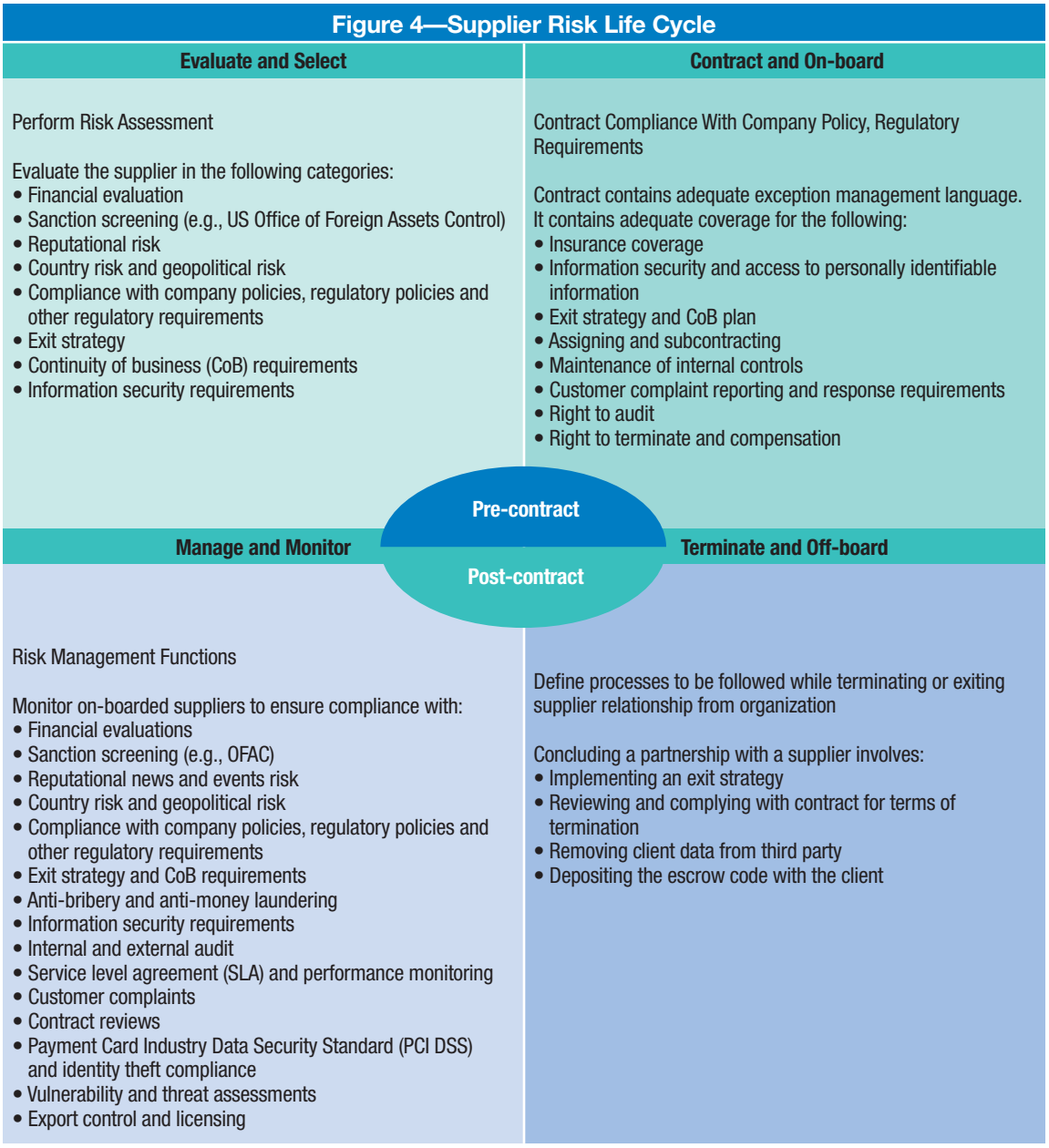
Supplier risk factors must be identified, monitored and managed across the supplier life cycle (during both the pre-contract and the post-contract stages) as they occur. Supplier risk determines the appropriate risk management activities at each stage of the supplier life cycle. **Figure 4** shows the steps in the phases of the supplier risk life cycle.

Emerging Areas

With the advent of the amplified stringent norms with respect to supplier risk management, the following categories of suppliers are now gaining importance and are gradually being brought under the regulatory scanner and ambit:

- Direct sales agencies and direct sales representatives
- Financial asset management companies

Figure 4—Supplier Risk Life Cycle



Source: S. Vyas. Reprinted with permission.

- Law firms supporting mortgage default/collection services
- Agent banks
- Accounting and audit services (unless they do not have substantial access to confidential customer information)
- Fourth parties/subcontractors
- Suppliers providing record management services

Conclusion

Dependence on suppliers and outsourcing is increasing day by day and so is exposure to risk. Without learning to identify, monitor and manage these supplier-related risk factors, organizations may face a bleak future given the continual increases in competitive edge among emerging competitors and regulatory oversight.

By having a strong foundation, organizations that have multiple supplier relationships can better manage and mitigate risk and losses (fines, noncompliances, reputational losses) as a result of supplier breaches and noncompliance.

Endnotes

1 Consumer Finance Protection Bureau, bulletin, 2013-13, 2012-03 and 2012-06
2 Office of the Comptroller of the Currency (OCC), "Risk Management Guidance," OCC Bulletin, USA, 2001-47