HELP
SOURCE
Q&A

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2OpBRTx

Q Is there any standard or framework for managing IT vendors? What best practices should we adopt to effectively manage vendors?

A Although IT vendor management has been an issue faced by many organizations, there is no specific standard or framework currently available for managing vendors. There have been many articles and white papers published to discuss various topics related to vendor management. ISACA® provides an excellent framework for enterprise governance of IT (EGIT), which includes vendor management.[1] Though the name of the book implies that it is meant only for organizations using COBIT® 5, it is very good guidance on vendor management for all organizations.

Outsourcing has its benefits, but also has associated risk. A point to be noted is that organizations outsource processes, not accountability. Therefore, managing vendors and their performance in accordance with business expectations is of primary importance for business management.

Due to the proliferation of IT, vendors are more like business partners who share equal or more responsibility for the organization's performance. Answers to the following questions help to establish the importance of vendor relationships to the organization:

- **How important is the vendor to the organization?** The answer depends on the criticality of the outsourced processes, the nature of outsourcing and dependency of the organization on the vendor.
- **How important is the enterprise to the vendor?** The answer depends on the positioning of the organization in the business sector in which the organization operates and the value, volume and duration of the contract.

Depending upon nature of outsourcing, there can be four categories of vendor:

1. **Strategic**—The vendor performs most critical functions for the organization such as data center management, enterprise resource planning (ERP) operations, etc.
2. **Tactical**—The vendor supplies process outsourcing such as call centers, service centers, IT operations, etc.
3. **Commodity**—The vendors are suppliers of materials such as office supplies and equipment, facility maintenance, etc.
4. **Niche**—The vendor supplies highly specialized products or services, for example, software or application development and maintenance, or implements complex solutions such as security information and event management (SIEM) or identity and access management (IdAM).

Generally, organizations use the services of all categories of vendors. Therefore, it is necessary to define and implement an organization-level framework for outsourcing governance. This framework needs to consider these enablers:

- **Strategy and policy**—Boards of directors (BoDs) need to define strategy for outsourcing. The basic principle is not to outsource core functions of the business. The policy also defines the minimum level of service and quality requirements within IT.
- **Governance and management processes**—Defining, rationalizing and standardizing processes across the organization is essential to ensure that processes are managed with the

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant in India.

optimal use of automated tools. The processes generally should include:

- **Determining requirements for outsourcing**—This needs to be defined at length to avoid ambiguity and confusion. Detailed requirements also help in defining service level requirements (SLR) and service level agreements (SLAs) for monitoring vendors once contracted.
- **Risk management**—Outsourcing risk management should follow the enterprise risk management framework. A list of generic risk that need to be considered will be given herein.
- **Steering committee**—A centralized steering committee for monitoring all vendors may be appointed at the top management level.
- **Selection criteria**—Vendor selection criteria may vary depending on the nature of outsourcing and assessed risk. There cannot be a uniform criterion for all vendors. However, defining minimum qualifications of vendors may be included in the process.
- **Acquisition process**—Outsourcing must be considered based on technical skills and competencies. It is appropriate to evaluate and select vendors based on technical competencies and, from among the vendors who qualify, commercial quotes may be considered. It is advisable that the organization work out minimum and maximum cost for required quality of technology and services before considering commercial quotes.
- **Contracting and SLA**—A contract execution is a legal process, and inputs from legal experts may be considered before drafting and accepting the terms of a contract. Generally, a contract is valid for a longer duration; however, the terms of SLAs may vary depending on business requirements. It is better to execute SLAs separately along with contracts.
- **Monitoring of performance and SLA**—The best practice may be to appoint an owner for every outsourcing arrangement who is responsible for monitoring the performance of the vendor and reporting to the vendor steering committee. The owner should ensure that issues are discussed and resolved to ensure user satisfaction.

"SINCE IT SERVICES HELP IN AUTOMATING BUSINESS PROCESSES THAT DELIVER SERVICES TO CUSTOMERS AND STAKEHOLDERS, MONITORING SERVICE DELIVERY MUST BE CONSIDERED A PRIORITY."

- **Governance**—The key aspects of governance in vendor management include measuring the value delivered by vendors and relationship management, which is the responsibility of the vendor steering committee. Some of the critical factors to consider include:
  - Analyzing the information using qualitative and quantitative vendor performance metrics with various stakeholders. This may be done on a monthly or quarterly basis.
  - Knowing what is being monitored, especially when monitoring vendor performance. Vendors often prefer to monitor technical performance (e.g., uptime requirements or timelines for delivery). But since IT services help in automating business processes that deliver services to customers and stakeholders, monitoring service delivery must be considered a priority.
- **Inventory and categorization of vendors**—Maintaining a centralized inventory of vendors and categorizing them helps ensure effective governance. The following activities can help in the categorization of vendors:
  - **Assessment**—Identify the nature and level of outsourcing. Many organizations outsource various activities. Some are controlled by the corporate office and uniformly deployed across geographies, while others are decentralized and managed by regional/local offices.
  - **Relationship**—Categorize the relationship with the vendor. Relationships with vendors can be strategic (e.g., for the organization), tactical (e.g., process outsourcing), commodity-related (e.g., suppliers of material) or niche (e.g., software development).
  - **Nature of outsourcing**—Understand the relationship with the vendor. The relationship depends on the cost of outsourcing, the value

received from it, the impact on the business, the length of the relationship and the ease of substituting another vendor.

Risk Associated With Outsourcing

Depending on the nature of the business and the extent of outsourcing, risk scenarios may vary from organization to organization; however, there are a few general risk scenarios that need to be considered while assessing vendor-related risk:

- **Risk associated with information security**—Organization may have implemented appropriate security, but the vendor systems might be vulnerable.
- **Risk associated with compliance**—Organization may have to comply with legal and regulatory requirements; however, vendors may not be aware of the same, resulting in noncompliance issues.
- **Risk associated with financial sustenance of vendor**—Vendors may have issues managing their finances, resulting in inadequate resource availability and, therefore, inadequate performance of contracted work. If this is not managed properly, a vendor may not be able to continue providing services, resulting in nonperformance by the organization.
- **Risk associated with operations**—A major objective of outsourcing is to take advantage of vendor skills and competencies in executing operations. These operations must be focused on achieving business objectives. Vendors need to understand them and align the performance of resources. Organizations must define SLAs based on these objectives. Risk materializes when there is gap in this understanding.
- **Concentration risk**—Organizations may select one vendor for all IT operations, thus increasing dependency on one vendor. Nonperformance to meet organization objectives or failure of one vendor will jeopardize the organization.
- **Compliance-related risk**—Organizations may need to comply with various legal and regulatory requirements. Although responsibility can be delegated to a vendor, accountability remains with the organization. To ensure compliance by the vendor, include provisions in the contract or SLA. Organizations need to establish a process for reviewing vendor compliance and, if required, auditing the vendor for compliance. This may be achieved through periodic audits. However, often, organizations do not appoint auditors due to various reasons such as costs or a vendor's concern about facing multiple audits. In such situations, organizations may ask a vendor to provide audit reports on service organization controls (SOC)—SOC 1, SOC 2 and SOC 3 performed as per Statement on Standards for Attestation Engagements (SSAE) 18 requirements.

It is important to note that vendor management is not a one-time activity. It is a continuous process that calls for sufficient and effective commitment from management in terms of governance and reviews to derive maximum benefits from the relationships with vendors.

Endnotes

1 ISACA®, *Vendor Management Using COBIT® 5*, USA, 2014, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Vendor-Management-Using-COBIT5.aspx*