June 2011

The Outsourcing Relationship

Effective service provider engagements involve up-front planning and active, ongoing management.

Richard Mosher, CISA, CISSP, CBCP, CGEIT
Risk Advisory Services Professional
Experis

Denise Mainquist, CISA, QSA
Managing Director
ITPAC Consulting

In today's business environment, outsourcing processes to a third party has become relatively commonplace. The practice gives organizations an opportunity to gain efficiencies, improve performance, lower costs, and focus on core competencies. Many businesses, however, fail to complete necessary due diligence work before the outsourcing relationship begins and neglect to take sufficient care of the relationship, adopting an "out of sight, out of mind" approach once outsourcing begins.

Successful outsourcing is no different from any other business relationship — it requires nurturing and management so that the needs of all parties are met. It is critical that both the purchaser and the supplier of outsourced processes understand each other's expectations and dependencies, as well as focus on maintaining a strong communication channel. Regular monitoring and reporting, for example, provide valuable information on the health of the relationship. Moreover, the organization needs to consider carefully any risks involved in the outsourcing engagement and perform necessary up-front planning in advance of vendor selection. Internal auditors play an important role in making sure risks have been addressed and verifying that the necessary steps have been taken to ensure the outsourcing relationship is successful.

THE RISK OF OUTSOURCING

An organization might outsource numerous activities to a third party: IT services and infrastructure, help desk services, and transaction processing, to name just a few. And although these arrangements have the potential to deliver significant value, the organization typically has little or no control over the service provider's internal processes. Consequently, any organization that decides to outsource part of its operations puts its reputation, along with any data processed or customer interactions performed on its behalf, in the hands of a third party.

Continued…

Successful outsourcing involves balancing the risks and benefits of obtaining external expertise in support of a set of tasks that are beyond the capabilities of internal staff or cannot be performed cost effectively in-house. And while a decision to outsource may help offset identified risks, the ultimate responsibility for effective performance of the function and for compliance with legal and regulatory requirements still resides with the organization. Moreover, The Committee of Sponsoring Organizations of the Treadway Commission's *Enterprise Risk Management–Integrated Framework* does not allow for risk associated with an outsourced process to be assumed by the service provider. Instead, the risk can only be shared with that provider. In such an arrangement, the organization remains responsible for risks and is required to monitor the outsourced process to ensure risks are addressed appropriately. The service provider can assume only the operational component of risk.

The level of risk to the organization increases when the outsourced process or function involves key business operations for which adequacy and efficiency must be ensured. That level increases even more when outsourcing involves IT functions, as IT directly impacts financial reports and management of critical customer data. Moreover, risk levels climb still further when outsourced work involves the security and privacy of corporate information.

Causes of Relationship Failures

Numerous factors can cause an outsourcing arrangement to fail. A few of the more common reasons include:

Service failures. The service provider may not be able to provide the level of service or expertise required to meet the needs of the outsourcing organization.

Support conflicts. The outsourcing organization and its supporting service company may enter the relationship with different expectations regarding the services to be performed and the timeliness of those services. Such disagreements may reach the point at which the relationship is dissolved rather than continued.

Monetary considerations. When all of the costs involved in an outsourcing arrangement are considered, the resulting service may not be as cost-effective as anticipated. Consequently, the organization may bring the function back in house to save expense.

Language differences. A common complaint in customer-facing services is poor communication with support staff and an inability to achieve mutual understanding. This complaint also applies to relationships between staff members within the outsourcing organization and service organization staff members. Failure to ensure adequate understanding can in turn cause the outsourced function to fail or to lose some of the outsourcing organization's customer base.

Compliance gaps. An external support arrangement may be discontinued because of gaps in legal or regulatory compliance requirements, or by a public failure to meet compliance needs (e.g., a breach of the organization's network security). Such failures may be caused by numerous factors, including local cultural norms taking precedence over a legal agreement, technical failure on the part of service support staff, lack of appropriate oversight by the outsourcing organization's management, and unwillingness on the part of the vendor to meet the outsourcing organization's compliance needs. In all such cases, the vendor may not be able or willing to meet established requirements, and the parent organization might need to make other arrangements.

Core functions. Functions performed by an outsourcing service entail a degree of separation from internal functions. In some cases, organizations determine that they are unable to operate effectively because the organization no longer has control over the entire process. The organization subsequently may determine that the outsourced function is in fact a core business process that should be maintained in-house to improve operational efficiencies. The organization will then make the necessary investment in internal expertise and systems to take over the process involved.

Continued…

When considering the possibility of outsourcing a business or IT function, the organization should evaluate the risks associated with performing the activity or task in-house versus handling it externally. The organization also should examine business requirements and objectives. If the risks associated with performing a process in-house do not match the objectives set for the organization, and the degree of risk involved in outsourcing the process is acceptable, then external options may be an appropriate path to pursue.

KEY RISK AREAS

Understanding key areas of exposure associated with outsourced processes and developing steps to mitigate those exposures are critical to the outsourcing process. Whenever a relationship with a third party is formed, strong due diligence processes are necessary to gain confidence in the soundness of the business, including its training programs, management style, and insurance coverage. Still, many organizations fail to look beyond the potential return on investment for the outsourced process and consider the risks. While cost savings will always be a major factor in selecting a third-party provider, numerous risks may have a greater impact on the organization and its bottom line. The internal auditor should verify that all applicable risks have been identified and considered when making decisions related to the outsourcing service.

Reputation

When a problem occurs — and inevitably it will — the organization, not the outsourced firm, will bear responsibility no matter where that problem lies or who created it. If the organization has staked its reputation on exceptional customer service or rapid turnaround, for example, it should consider how these areas might be affected when direct control resides outside the core business. For instance, when an outsourcer provides help desk services, it acts as a customer interface on behalf of the organization. When providing back-end processing, the provider deals directly with the customer data on the organization's behalf. In both cases, the customer agrees to a relationship with the organization, thereby placing the organization's reputation at risk.

Strategy

Would outsourcing the process under consideration help the company meet its strategic objectives? If the process comprises back-office activities and can be performed by a vendor with greater expertise and resources, then outsourcing may allow the organization to better focus on its core strengths. If it involves a key business process, those responsible for the decision need to understand how outsourcing fits with company strategy. Moreover, the organization needs to determine the level of training and management that may be required to make sure the outsourced process works effectively and continues to support the strategy.

Compliance

Similar to reputational risks, accountability for compliance with specific regulations or industry standards — such as the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the Payment Card Industry Data Security Standard (PCI DSS) — cannot be outsourced. Merely asking vendors whether they will comply with a set of requirements is generally inadequate, because the answer invariably will be a resounding "yes," regardless of the vendor's actual intent or capabilities. Internal auditors should consider assessing whether the organization has clearly defined its expectations of the vendor, including any procedures it may be required to follow. Additionally, they should determine whether those requirements are being met through active management or monitoring of externally defined certification status, such as those associated with PCI DSS compliance.

Continued…

Security and Confidentiality

Organizations need to consider who has access to sensitive or confidential information and how that access affects compliance with regulations and policies. Those responsible for the outsourcing process should consider several issues, including:

Will the vendor limit its employees' access to sensitive information?
Is information stored at a vendor site? If so, is every storage location known to the outsourcing organization?
What controls and security practices does the vendor enforce to provide assurances that critical information is handled appropriately?

To obtain more direct insight on how the vendor handles sensitive information, organizational decision-makers should also ask the vendor to supply any certifications or outside assessment reports for audit review.

Organizational Structure and Composition

An organization's structure, size, and staffing can play critical roles in the success of an outsourcing relationship. Vendors that can react quickly to a change in requirements or address an issue rapidly, for example, can offer an advantage in meeting certain needs. However, this same nimbleness of response can be detrimental if solid controls and activity reporting are required for regulatory purposes, as the vendor may compromise in these areas to achieve efficiency. In addition, differences in internal reporting structures between the company and the outsourcing provider can lead to long-term conflicts if not recognized and addressed early in the process. For example, an outsourcing provider may have a decentralized and informal security structure, which can be problematic for an organization that requires a more formally structured approach to information security controls. Small service providers may be more responsive to the organization's needs because they value the organization's business, but responsiveness may decrease if they have inadequate staffing levels to support operational needs. Formalized processes within larger or more mature outsourcing organizations can help support compliance and reporting needs, but can also slow responsiveness if not optimized. Staff turnover within the provider firm and an inability to retain staff experienced in the background and requirements of the company can also impact the success of the outsourcing effort.

Ongoing Relationship Management

Any organization that outsources business or technical functions must actively manage the relationship. Internal auditors should consider taking the following actions to ensure ongoing vendor management efforts are effective:

1. Confirm the current legal and regulatory environment of the organization, and its impact on the vendor agreement.
2. Understand the risks introduced through the vendor relationship, or risks that are inherent in the contracted organization or outsourced process. Ensure there is an ongoing risk assessment process and that high-risk outcomes are mitigated appropriately.
3. Gain an understanding of the existing internal controls pertaining to the contract.
4. Gain an understanding of the vendor organization and any changes since the previous audit.
5. Obtain and review copies of any vendor-operations and user manuals related to the services provided to the organization.
6. Obtain and review copies of any third-party or internal audits of the vendor related to the services provided to the organization.
7. Confirm that the services provided meet the organization's expectations as defined in the service-level agreements.
8. Verify that expenses incurred are appropriate based on the services provided, contracted costs, and service-level agreement requirements met. This process must include verification of vendor expenses through validated reporting procedures.

Continued…

9. Either through a third-party review or an internal assessment of control processes, confirm that vendor controls aimed at protecting the services provided to the organization function effectively.

10. Ensure that the organization follows up with vendors to provide feedback on their services and level of compliance as established through the vendor assessment process.

For additional information and guidance related to vendor management, see The IIA's Practice Guide, Auditing External Business Relationships.

Key Processes

Increasingly, companies decide to outsource key business processes to meet specific strategic objectives. A key process is one that is central to the services a business delivers and has a direct effect on organizational success, such as transaction or claims processing. When a key business process is outsourced it falls into a category of service provider called business process outsourcer (BPO). There are many potential advantages to outsourcing to a BPO — such as improving client service, turnaround time, and profitability — because the company is able to focus on more strategic objectives and allow the BPO to handle day-to-day processes with greater efficiency and expertise. However, the potential risks when outsourcing a key process are greatly increased because the outsourcing company gives up a significant amount of control over how that service is delivered to customers.