

The Inside Story on Outsource planning

By Steven I. Adler, Prentice Robertson, and Kort L. Dickson

August 2005

Outsourcing continues to be an appealing strategy for business executives, who see it as a way to cut costs and focus the company on core competencies. Security is frequently one of the functions selected for outsourcing. More than half of the respondents to the 2004 ASIS salary survey said that their companies had contracted out some portion of security services. But contracting won't meet corporate objectives unless the process is properly managed. The key to success is to have a plan for every step of the project, including not only how the vendor will be selected, but how it will be integrated into the company's operations. A good model to follow is known as contract lifecycle management (CLM), which consists of four primary components: contract governance and oversight, request for proposal (RFP), due diligence, and contract negotiation and execution. These elements provide a disciplined approach for optimal vendor selection and consistent contract performance.

Governance. The first step of the process is to form a contract governance and oversight council. The council should include representatives from the leadership of the organization's core business segments and functions, such as contracting and procurement, legal, compliance, finance, human resources, operations, and information technology. By involving this cross-section of management in the CLM process, the company can identify all of the business and system requirements that any contract service suppliers will have to meet.

The council should secure senior management buy-in at the beginning of the outsourcing process and reinforce it throughout the resulting program's lifetime. The council should encourage corporate leadership to take an active role in all phases of the CLM process from exploratory discussions to monitoring for compliance with the contract.

In one case, General Nutrition Incorporated (GNI), where author Adler previously worked, wanted to outsource its employee background checks to reduce operational costs and turnaround time, as well as to create a standardized approach to employment hiring practices. GNI had a governance and oversight council that spearheaded the process, ensuring that all business interests would be addressed up front.

As part of GNI's governance and oversight, the human resources and legal departments first looked at company expectations, which were to find a vendor that could verify the employment and education of any new hire and to review credit and criminal records. The legal representative also assessed vendor compliance with relevant state employment laws. Meanwhile, the governance and oversight IT representative made sure that the selection process would address issues of system connectivity between the company's personnel and the vendor's database.

RFP. The second step of the process, the request for proposal (RFP), begins with a team of corporate stakeholders who develop a detailed statement of work (SOW), which can be thought of as painting a picture of a process landscape.

A SOW takes the form of a narrative description of products and services to be supplied, or tasks to be performed by the vendor, under a proposed contract, including equipment and capacity needs and required outputs. This document should also consider operational processes, system and data requirements, human resource demands, and the turnaround times associated with vendor output.

For example, a retailer outsourcing the analyses of its point-of-sale (POS) exception-based reports would have to identify all data feeds from its stores to the central IT servers, data capacity requirements, maintenance needs,

and—most importantly—it would have to determine what data was to be captured, trended, and formatted for management reporting.

The RFP and SOW should include an outlay estimate—basically the amount the company is willing to spend for the service. This might be a range or a cap above which vendor proposals won't be considered. The RFP and SOW should also include a discussion of performance incentives, if any, that would affect the total compensation package to the vendor.

For example, when GNI moved to outsource its background verification services, GNI explained in the RFP and SOW what it would offer in terms of incentives and what it would require in terms of performance guarantees. GNI expected a three-day turnaround on each check. If the vendor completed the checks in less than three days for one month, an incentive payout to the vendor would be made.

The RFP and SOW also address service-level agreements, which encompass service or product delivery requirements, including timeliness and quality expectations. Additionally, the RFP includes a service-monitoring process, with quality measurements, and it should spell out how problems would be addressed through an escalating series of communication and quality-remediation steps.

Due diligence. A contractor's past performance record is the key indicator for predicting future performance. Thus, a detailed inquiry into prospective vendors is necessary to ensure their operational and financial soundness, transparent ethical standards, and ability to meet company service requirements.

A due diligence team should be assembled, with representatives from functional areas that will work with the selected service provider, such as human resources, legal, and finance. Since the due diligence process requires a high level of confidentiality and expertise, a consultant or "of counsel" legal advisor should be brought in to manage the process.

The due diligence process should begin with a request for information (RFI)—a detailed questionnaire to the vendor's chief executive and financial officers. The questionnaire should ask for specific information associated with the vendor's operations, including financial statements and regulatory-compliance documentation that shows how the company complies with applicable federal and state requirements, such as Sarbanes-Oxley.

It should also ask for information on pending litigation and potential mergers or acquisitions. In addition, the questionnaire should request other pertinent documents, such as letters of credit and Standards of Auditing Statement-70 reports that are associated with certification of the controls on the vendor's business and system processes by external auditors. Other requested materials would be licensure requirements, proof of adequate bonding and insurance, and a client list from which a random sampling can be contacted.

Supplemental to reviewing all of that information, the due diligence committee should perform an on-site visit and vendor interview. During the visit, committee members should be able to deduce an important indicator of suitability—the vendor's investment in its people, property, and equipment. For example, if officers' uniforms are unkempt and the patrol vehicles appear shoddy, the vendor should be eliminated as an outsourcing candidate.

During the interview, the committee members should once more explain the company's expectations of quality, service-level agreements, costs, and contract enforcement requirements so that the potential vendor is clear about the expected service standards.

The governance and oversight council should then assess the information from the due diligence committee to narrow down the finalists. If needed, the council should have the due diligence committee ask further questions to clarify vendor information. By the end of this process, the best choice should become clear.

CNE. Contract negotiation and execution (CNE) is the last phase of the CLM process. This is when the hiring company and the selected vendor agree on final terms, document them, and execute the contract. As a part of this process, a contract negotiation team should be formed from a cross-section of internal stakeholders to review the contract for accuracy and appropriateness.

For example, if the company is outsourcing guard services, the chief security officer should ensure that staffing coverage is adequate for emergency response and around-the-clock operations, including duties such as escorting. Similarly, the chief risk officer should review insurance coverage levels and risk riders to ensure that they satisfy corporate requirements. These parameters would already have been discussed and reviewed by these people in preparing the RFP, but this final review ensures that nothing has been overlooked before the contract is signed.

There should also be a contract review by the legal department to ensure that the contract is binding on all parties. Finally, there should be a review and approval by the chief financial officer and an acceptance of the contract.

Facing change. Once the contract has been signed, the company must prepare itself to manage the change. Three key elements in a successful transition are a dedicated transition team, focused communications with affected employees, and a transition analysis, including monitoring of performance indicators.

Team up. It is important to create the right team to oversee and manage the transition. Members should be chosen based on a variety of factors, such as their ability to work collectively, their stature in the organization—whether formal or informal—and their ownership over individual pieces of the security function. A team might be composed of managers from human resources, operations management, maintenance or facilities, and information systems, and front-line staff with a reputation for being peer-group leaders.

If there have been any major detractors of the program, it makes sense to invite their participation. The more they get involved and have a sense of ownership in the project, the more they are likely to want it to succeed.

Many guard service providers tout the ability to provide customers one point of contact—a single manager to provide all the answers, oversee the operation, and run the account. Although this may be viable with small accounts, it is not a realistic solution for any significant transition.

New providers should, therefore, be prepared to furnish a significant management presence throughout the initial transition time to ensure that the new officers are operating at acceptable levels and that any deficiencies are addressed in a timely manner. This issue will have been addressed as an expectation in the RFP and SOW.

Communication. The transition team must be prepared to explain to the affected personnel the reasons behind the shift to outsourcing, the specific timing of events, the extent to which services important to the receiver may be affected, and most importantly, how questions or other issues will be managed throughout the transition and under the new arrangement.

For example, when one company hired a guard service, the transition team sat down with the manager to explain changes and to make sure the manager knew that he could bring any problems or questions straight to the team for resolution.

In another case, a company that had experienced sabotage at a Midwest manufacturing plant outsourced the resulting investigation. During the CLM process, the vendor told the company that company personnel would be significantly involved in the investigation. If focused communication had not followed between the company and its support personnel, those employees may not have been available or able to provide the level of assistance the investigators required.

Transitional analysis. After the process is complete, the transition team must carefully examine any new procedures, including those for daily activity reports, exception reporting for alarm activations, handling of procedural violations, publishing of schedules, training methods, planned management interaction, inspection forms, and emergency communications.

The transition-analysis process allows team members to assess how well the new procedures are working and, where needed, to make changes. This process will ensure that the services provided are achieving the desired outcomes. The team's involvement in fine-tuning these procedures will also create ownership of the process and, ultimately, wide support throughout the organization.

At a Chicago distribution company, for instance, the lack of available receiving docks often led to a backup in deliveries, causing employees to work too much overtime. During the transition analysis, it was discovered that a new contract swing officer who roamed between the shipping and receiving areas had ample time to redirect incoming vehicles to available shipping docks.

This arrangement had not been anticipated at the time that the RFP and SOW were worked out. But the analysis after the contract work began revealed the opportunity for this improvement.

By having the roaming officer communicate directly with the transportation manager about the loading dock traffic and availability, the company was able to unload deliveries in a timely manner with little or no employee overtime. It also allowed the officer to become familiar with the drivers, vehicles, and shipping and receiving processes, adding security value where none existed before.

KPIs. Contract provisions usually require that vendors document and report key performance indicators (KPIs). During the transition phase, it is important that there be close monitoring of KPI measurements and other daily performance indicators to see both that the information is adequate and meaningful and that the performance is meeting expectations.

During the transition, the regular cycle process of reviewing performance should be shortened to monitor individual performances and functional duties that are vital to the operational success. That way, any problems can be caught early and addressed.

Outsourcing will continue to be a favored business strategy. Security managers who take a lifecycle-management approach to the contracting process will be most likely to achieve the desired result.

Steven I. Adler is business risk manager with Uniprise of West Hartford, Connecticut. Prentice Robertson is executive vice president of St. Louis-based Whelan Security. Kort L. Dickson is senior manager, global security, for Kraft Foods of Northfield, Illinois. All three are members of the ASIS Business Practices Council.

Security Management is the award-winning publication of ASIS International, the preeminent international organization for security professionals, with more than 35,000 members worldwide.

ASIS International, Inc. Worldwide Headquarters USA, 1625 Prince Street, Alexandria, Virginia 22314-2818
703-519-6200 | fax 703-519-6299 | <http://www.asisonline.org/>



Copyright © 2008, Security Management

Source URL: <http://www.securitymanagement.com/article/inside-story-outsourcing-planning>