Imagine asking two teenagers to take out the garbage every Wednesday. Anyone who has kids knows that the garbage will not be taken out on Wednesday because the two teenagers will point at each other and say, “I thought he/she would do it.” In an environment where IT is outsourced to multiple service providers, IT struggles with a similar challenge. For example, when one has a complex incident that cripples a major business aspect, the suppliers will inevitably point at each other and say “it’s their fault.”

**VENDORS NEED TO WORK TOGETHER**

“The biggest single mistake in multivendor outsourcing agreements is that companies don’t take into account how the vendors will have to work together,” said Frank Casale, the founder and chief executive officer of the Outsourcing Institute.

Individual contracts cannot typically cover all activities and possibilities of technology or process issues that can happen along the service chain (see figure 1). If the suppliers do not cooperate, the sum of the discrete service levels will most likely not reach the desired end-to-end service level.

High-level governance models are appropriate for board rooms and executive discussions, but often fail to convey the message of how the vendors need to cooperate to provide IT services to the client. The key to achieve the necessary cooperation and to reach productivity-enhancing end-to-end service levels is to recognize the need for (1) a guardian or a service integrator, and (2) a framework for cross-supplier procedures.

**OUTSOURCING AND DECREASED CONTROL**

Companies increasingly use more multisupplier sourcing with the intent to access best-in-class capabilities and improve their negotiation position. In a recent survey by Deloitte Consulting LLP, 29 percent of interviewed executives said they used multiple service providers. Chief information officers find that as they use increasingly sophisticated solutions from their multiple suppliers, they have less control. Thus, the control of a multisourcing environment through governance processes becomes more and more relevant.

So, in the face of reduced control, why is there an increasing move toward multisourcing arrangements in outsourcing engagements? The answer is that different IT service providers have different strengths and capabilities and cost structures. Often, service providers have strengths in specific industry segments (e.g., health care, automotive) or with particular products or technologies (e.g., SAP R/3, network management) and have built up the skills and the knowledge to provide strong value in that particular area. In addition, companies with good application support (apps) sometimes have relatively weak infrastructure or operations (ops) support under the same roof, and vice versa. One of the reasons for this phenomenon could be that

---

**Figure 1—Service Chain**

<table>
<thead>
<tr>
<th>Service Provider A (e.g., app hosting)</th>
<th>Service Provider B (e.g., WAN provider)</th>
<th>Service Provider C (e.g., local LAN)</th>
<th>Service Recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Level A</td>
<td>Service Level B</td>
<td>Service Level C</td>
<td>End-to-end Service Level</td>
</tr>
</tbody>
</table>
apps are more a people-focused endeavor (because most of the cost of apps is people) than ops, which results in different types of corporate culture. Labor arbitrage or “cost-shoring” (i.e., finding the best geographical location for the service) in most instances can be more appropriate for apps than for ops. In infrastructure outsourcing, there is often less room for cost-shoring as one deals with hardware and tools (e.g., networks, servers, monitoring) rather than people.

The consequence of the service providers having different geographical structures and strengths is a differentiation in cost and value or “bang for the buck.” The incentive to multisource comes from the desire to optimize the value propositions that different IT service providers offer. The overall result is that, conceptually, multisourcing makes sense and can improve service levels and save money.

However, the practical implementation of multisourcing is difficult because of governance issues. Adding multiple suppliers in diverse geographies and disciplines increases the complexity and the points of potential IT failure. An example of potential failure is when a change in an application (e.g., a new release or a patch) is implemented. Coordinating such a change with ops people is logistically difficult, because apps and ops are typically separated and reside in different IT “towers” or “silos” or “stovepipes.” They have a different vocabulary, different mentalities, different tools, different priorities, and they report to different bosses. Now, add two or three different continents into the mix. It becomes obvious that these complex situations require a smooth hand-off and interface from one supplier to another to reduce the finger-pointing and control the overall challenge of outsourcing in a multisupplier environment.

**GUARDIAN OR SERVICE INTEGRATOR**

The saying goes that “triangles belong in trigonometry, not in marriages.” Similarly, triangles in IT with one client and two suppliers, or more, seldom work well. It would be naive to think that suppliers will work “nicely” together when profit margins and jobs and bonuses are involved. Whatever work is not done by one supplier will need to be done by another supplier, and outsourcing contracts do not typically go into enough granular detail of the IT activities to ensure that all possibilities are covered. In addition, the outsourcing contracts typically do not provide enough profit margin to allow for major unbudgeted activities. The cost constraints underscore the need for thorough coordination of any activities that are shared among suppliers. The coordination is often called “aggregation” or “integration” management. Some companies call it the “guardian” role or the “service integrator.” The role of integration management (see **figure 2**) is to ensure end-to-end service levels and the designation of the related accountability and responsibility for any activity that involves a hand-off between suppliers.

The traditional way of dealing with integration activities is to incorporate them into the internal vendor management
function, because this function often contains procurement and legal knowledge and is hence more prone to be a “referee” for disputes between suppliers. However, vendor management does not usually contain the technical and operational expertise to deal with integration activities.

The knowledge and experience needed for integration activities can be difficult to build and retain internally and is often found in specialized groups within outsourcing service providers. Integration activities are more often than not noncore to the client’s business, and the integration or guardian role itself becomes a target of outsourcing. Vendor or supplier management, including integration activities, can be partially or completely outsourced.

The purpose of the guardian role is to provide a single body responsible for the delivery and end-to-end management of the IT services in a multivendor environment. In IT Infrastructure Library (ITIL), the guardian role is described as a “product manager”—owning a service end-to-end, even if multiple vendors are involved. The genesis of the role was clients who articulated the following requirement for the prime vendor: “Make sure the fragmentation of the IT services—caused by multiple service provider contracts—will not have a negative impact on the end-to-end IT services delivered to us.”

Typical activities for the internal or external guardian or integration manager are to:

- Produce, review, own and maintain content of global service level agreements
- Provide process audit, management, monitoring and quality assurance functions for adherence to contractual obligations
- Assume end-to-end responsibility for service level management
- Create corrective actions and manage service improvement programs
- Coordinate multiprovider high-priority incidents, root-cause analysis activities, release and intersupplier change management processes
- Communicate service recipients’ policies and standards and ensure that service providers comply
- Measure and monitor process effectiveness and compliance, and make recommendations for improvement

Most of the time, the guardian does not assume accountability or contractual liability for other vendors that contract directly with the client. This means the guardian does not absorb penalties or financial consequences for lapses in the vendors’ services. The role requires the guardian to function as the central point for all client service queries, and establishes the guardian as the primus inter pares—first among equally important suppliers.

The guardian function is the logical place for the accountability for end-to-end service levels. However, the contract between the guardian and the client typically does not dictate guaranteed end-to-end services to the client, but facilitates the resolution and pinpointing of any breaches in service levels. Hence, the guardian leads the restoration of service, rather than the client. Over time, the detailed operational knowledge required to do this quickly and effectively resides within the guardian.

The decision to outsource the guardian role is mainly a function of considering major pros and cons of keeping this role in-house (figure 3).

<table>
<thead>
<tr>
<th>Arguments in Favor of Keeping the Guardian Role In-house</th>
<th>Arguments in Favor of Outsourcing the Guardian Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undisputable end-to-end accountability and control</td>
<td>Easier for a specialized outsourcing service provider to build and maintain the broad technical and operational skill sets required for multisupplier coordination</td>
</tr>
<tr>
<td>Defining and negotiating a contract and service levels for an outsourced guardian role can be complex.</td>
<td>Predefined cross-supplier procedures</td>
</tr>
</tbody>
</table>

**Figure 3—Pros and Cons of Outsourcing the Guardian Role**

**CROSS-SUPPLIER PROCEDURES**

Cross-supplier procedures (CSPs) are a description of the operational interfaces between different suppliers to facilitate the end-to-end service levels required by the client. There is an intuitive understanding of the need for interfacing, communicating and agreeing on all operational activities.

In 2004, a Fortune 100 company announced a competitive negotiation of its US $15 billion master outsourcing contracts. The intention was to redistribute the outsourced work from one major supplier (single sourcing) to a set of big-name suppliers (multisourcing). The company found that none of the existing IT frameworks (ITIL, CMMI, ISO 27001, ISO/IEC 20000, CoBIT, etc.) provided a really efficient structure to enable airtight governance, where accountability and responsibility are completely defined across the IT spectrum. IT frameworks indicate partial answers, but the
The company felt that there is no such thing as a unified theory of IT governance. The company had to come up with its own solution, and a set of CSPs, managed by a guardian, was the operational key to that solution.

The output of its preparation for the massive outsourcing effort was an overall operational model, in which all relevant processes were described. For each process, a process definition document was made. The document provided details about process definition, subprocesses, roles and responsibilities in a RASCI chart, metrics, and "swim lanes" of the activities. To make the swim lanes practical and effective, the IT organization needed an additional layer of granularity and documentation to describe the interfaces and hand-offs between its suppliers. That layer was a set of CSPs.

**OPERATIONALIZING SWIM LANES WITH CSPS**

CSPs can be defined as the set of procedures describing the arrows where they cross the lines between activity swim lanes. Basically, CSPs are a written set of mutual expectations around the hand-offs occurring between different suppliers in a multisupplier outsourcing environment.

In Figure 4, it is assumed that the different lanes are "owned" by different entities. In this example, the service recipient (top lane) is the end user. The bottom lane represents the activities of the integration manager or the guardian. The numbered circles (1, 2, 3 and 4) pinpoint where the CSPs are defined, as this is where the hand-off occurs between different suppliers.

For each point that crosses a swim lane divider, a supplier is found on both sides of the dividing line. So, for each crossing point, one needs to describe what happens at that particular interface:

- Description of the hand-off action
- Deliverable (e.g., document, report, filled-out template)
- Technology aspects (e.g., batch vs. real-time updates, network links)
- Data variables (e.g., required fields, formats, database updates)

**Figure 4—Swim Lanes With Hand-offs**
• Acceptance criteria (time, quality, scope)
• Metrics around the hand-off (e.g., timing requirements)
• Cost aspects

This information can be captured in a simple document template, as is shown in figure 5. The document can also contain contact names, escalation aspects and arbitration procedures in case of disputes.

In a football match, a referee is needed to control the game and the players. Similarly, some organizational function is needed to control the CSPs. This control function can also be outsourced, but it ultimately needs to be managed by the customer or its substitute, the guardian.

CONCLUSION

The combination of the guardian role and the CSPs applies the principle of having a single point of accountability for any particular activity, thereby ensuring accountability and responsibility for that activity. The CSPs remove any excuse for a supplier to point at another vendor and say “it’s their fault.” Because CSPs enable the execution and proper functioning of the workflows depicted in the swim lanes, they represent the bridge between the theory of multisupplier governance and its practical execution.

With well-defined governance and CSPs, the garbage will be out on Wednesday.

AUTHOR’S NOTE

The author would like to thank to Kamal Dave, Mitch Kenfield, Dalibor Petrovic and Randy Steinberg for their input, comments and advice.

ENDNOTES

1 Jeanne Ross and Peter Weill (MIT CISR) define IT governance as “the organizational distribution of the decision rights and accountabilities to encourage desirable behavior in using IT” (HBS Press, 2004). Their definition implicitly underscores the importance of designating accountability if one wants results.


<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Service Recipient</th>
<th>Service Manager (SM)</th>
<th>Service Provider 1</th>
<th>Service Provider 2</th>
<th>Method</th>
<th>Timing</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Service desk (SD) receives call that service is disrupted (or complaint).</td>
<td>O</td>
<td>R</td>
<td>Phone; e-mail; SD system</td>
<td></td>
<td>Start (T=0)</td>
<td>Calls from service recipient can be user or business. SD provides both telephony and terminal input capability.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>A service provider detects an incident impacting the service recipient, assigns priority and provides incident information for record initiation to the SD.</td>
<td></td>
<td>R</td>
<td>O</td>
<td>(tool interface; SML)</td>
<td>Start (T=0)</td>
<td>Contact list of service provider is at <a href="http://www.fictionalcompany.com/intranet/repository">www.fictionalcompany.com/intranet/repository</a>.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Integration manager detects an incident from its operations monitoring, assigns priority and provides incident information for record initiation to the SD.</td>
<td></td>
<td></td>
<td></td>
<td>(Tool interface; XML)</td>
<td>Start (T=0)</td>
<td>Integration manager assigns priority and starts high-priority incident notification and escalation if priority is 2 or higher.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Service provider (for a SP-detected incident) or RSD (for a User-detected incident) forwards high-priority incidents to integration manager.</td>
<td></td>
<td></td>
<td></td>
<td>Paging System Duplicate</td>
<td>Timing to notification &lt; 15 minutes</td>
<td>Integration manager audits (quarterly) congruence and overlap of notifications from service providers and SD.</td>
<td></td>
</tr>
</tbody>
</table>
This argument is becoming less valid, because of remote monitoring capabilities, cloud computing, Software as a Service, etc. Also, select aspects of ops (e.g., the help or service desk) can be very labor-intensive.


Ibid.


RASCI stands for Responsible, Accountable, Supporting, Consulted and Informed. The acronym RACI (without the “S”) is more common and found in CoBiT.

An extensive discussion about the optimal usage of “swim lanes” can be found in the seminal work of Geary Rummler and Alan Brache, Improving Performance, Wiley, 1995.