IT Governance and Outsourcing

By Hugh Parkes, CISA, FCA

IT governance is a subset of corporate governance. It refers to how well an organisation governs or controls those of its activities that involve the use of information technology. In both business and government organisations, there are now few key activities that do not involve the use of IT as either an enabler or an intrinsic part of the capacity to allow the activity to take place. It should be stressed that IT governance refers to how the entire activity using IT is controlled—not just the IT department or the physical manifestations of IT, but the business knowledge and information that the activity requires for its successful operation.

Outsourcing, in its most common form, involves the contracting out of one or more of an organisation’s activities to an enterprise outside the corporate or government bounds. Activities of many types can be outsourced. The form of contracts or agreements that set the parameters under which the outsourced activity will be carried out can also vary considerably. Properly constituted organisations have the capacity to enter into contracts with one another, and many legal endeavours go into working out the terms of the contract, as well as assessing how its terms are complied with during the duration of the contract. However, the leaders of the organisations entering into an outsourcing agreement need to ask if their experience in reality delivers the objectives they have set for themselves in making the strategic decision to outsource or to provide the service now outsourced.

IT Governance Perspectives for Organisations Outsourcing Activities

The perspective of executives or directors toward the need for effective IT governance depends on how important the activity or resource provision outsourced is in the context of achieving the organisation’s strategies. If what is outsourced is a replaceable commodity or service, then problems can be overcome by going to an alternative supplier with low transfer risks. However, if what is outsourced is vital for the organisation’s ability to operate, then IT governance considerations and the frequency of reporting on service delivery and effectiveness of associated performance become of high importance. Figure 1 sets out types of activities that can be outsourced, the risks associated with outsourcing such activities and what IT governance issues should be considered.

<table>
<thead>
<tr>
<th>Outsourced Activities</th>
<th>Risks From Outsourcing and Possible Consequences</th>
<th>IT Governance Considerations for Executives and Boards</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Outsourced information management and storage (all value stored, databases, customer files, key parameters, etc.)</td>
<td>Very high risk—Depending on how critical the information stored with the outsourcer is • Consequences of loss or unauthorised access via penetration or poor security • Immediate impact, meaning this instant • Exposure to a wide spectrum of risks, e.g., loss, theft, integrity corruption, competitor access • Outsourcer negotiating power through organisation dependence on continuing access</td>
<td>• Ensure the outsourcing contract covers acceptable access rights and clear ownership of information. • Ensure adequate backup and disaster recovery arrangements have been made. Executives should cite specific evidence of successful recovery testing. Directors should request from CEO written confirmation that this test has taken place. • Inquire as to security over information stored and communications channels with access to the information. • Inquire as to information management effectiveness (how it is stored, how it is used, what management reports are derived from it and about its condition—this is where the organisation’s value is stored). • Inquire as to the extent of information mining in use, information architectural fit with organisation’s needs, and level of integration of related information for process effectiveness. • Ensure that the cost of outsourced service and the level of service received meet strategic needs.</td>
</tr>
<tr>
<td>Outsourced Activities</td>
<td>Risks From Outsourcing and Possible Consequences</td>
<td>IT Governance Considerations for Executives and Boards</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2. Outsourced core knowledge systems and development of new, or maintenance of existing systems (corporate memory, key knowledge elements, activity processes, executive preferences, etc.)</td>
<td>High to very high risk—Depending on how critical the outsourced knowledge systems are to the organisation's strategic operations • Exposure to a wide spectrum of risks, including intellectual property theft, process integrity corruption and competitor access • Dependence on an outsourcer to develop new systems and/or associated intellectual property can mean extreme vulnerability or loss of credibility.</td>
<td>• Ensure adequate backup and disaster recovery arrangements have been made (as noted previously). • Inquire as to security over system stored on the outsourcer's servers or in its computer installation. • Inquire into how systems access information is stored by outsourcers and the security of associated communication channels. • Inquire as to the level of the organisation's dependency on the outsourcer for development or maintenance of new or existing software; understand where knowledge and necessary competencies covering systems now reside—it may now be in Bangalore rather than San Jose. • Inquire as to project delivery management for new systems. • Inquire as to system uptime and maintenance performance, e.g., is the IT engine being adequately maintained? • Ask if the contracted service and uptime operational commitments are being met by the outsourcer.</td>
</tr>
<tr>
<td>3. Outsourced major computer installation and ancillary support services</td>
<td>Medium to high risk • Establishing major data centres run by major outsourcers should lower risk via economies of scale, experience, sound data centre procedures, and depth of supporting services. • Organisation outsourcing needs to ensure that outsourcer's installation is soundly run and contractually arrange access rights and verification arrangements (possibly via a third party such as a competent assurance provider). • Risks arise where outsourcing organisation does not monitor the service received or the ongoing condition of the computer installation on which it depends.</td>
<td>• Ensure adequate backup and disaster recovery arrangements have been made and tested (as noted previously) with participation or observers from the organisation onsite. • Inquire as to assurance reports on installation service and uptime performance. • Ask if the contracted service and uptime operational commitments are being met by the outsourcer.</td>
</tr>
<tr>
<td>4. Outsourced networks or communications</td>
<td>Medium to high risk • Risks include illegal or malicious penetration (hacking), denial-of-service attacks, information or system corruption, intellectual property theft, viruses, worms and Trojan horse attacks. • Alternate network routing capabilities must exist and have been tested for major networks so single point of failure dependency (bottleneck risk) is overcome. • Insufficient communications capacity slows processing or lengthens customer service centre response times.</td>
<td>• Ensure adequate backup and disaster recovery arrangements have been made and tested. • Inquire deeply as to security at all points of the network, extranets and intranets, as well as over links to the Internet, to Internet service providers (ISPs) and to the organisation's web site. • Inquire as to the adequacy of bandwidth or communication network capacity to the organisation, e.g., does it meet strategic needs? • Ask if the contracted service and uptime operational commitments are being met by the outsourcer.</td>
</tr>
<tr>
<td>5. Provision of computer equipment, replacement of network PCs and servers, network devices</td>
<td>Usually low risk • Alternate suppliers available • Contract does not meet commercial/entity needs over time. • Poor service is received leading to lower productivity or higher downtime. • Outsourced service provider does not keep equipment current.</td>
<td>• Comply with terms of outsourcing agreement (service received/payments made). (Issues arising are normally handled by entity middle management.) • Bring to executive or directors’ attention only if a disaster occurs, probably to seek recovery fund.</td>
</tr>
</tbody>
</table>

_Information Systems Control Journal, Volume 5, 2004_
Easy-to-Understand Reporting

It is usually possible to present clear reports to executives and directors in the form of overview flowcharts of outsourced activities with problem areas highlighted in colour (e.g., red for major IT governance concern area), as well as showing the linkages to activities that have not been outsourced. IT governance covers a wide range of risk issues as well as operational and commercial delivery issues. Some people find it much easier to get the “big picture” from a diagram rather than from long reports in technical jargon. If understandable reports are not being received at present by executives or directors, then IT governance issues can become a major corporate governance liability.

Figures 2 and 3 provide examples of reporting on IT governance in an overview flowchart form, allowing one to get the big picture on internal controls and security quickly, and to focus on what matters.

IT Governance Perspectives for Organisations Providing Outsourcer Services

The other party in an outsourcing arrangement is the outsourcer—the entity providing the original organisation with services. The outsourcer is the other party to the contract for service delivery, and has a different perspective to be considered for IT governance purposes from that of the receiving organisation. The differences are emphasised in figure 4.

Hugh Parkes, CISA, FCA

is a director of Parkes & Parkes, management consultants, based in Melbourne, Victoria, Australia. Parkes has extensive experience in IT consulting, banking and financial services, which has included the management of outsourced relationships as well as the provision of services as an outsourcer. A past member of the IT Governance Board, ISACA’s International Board of Directors and the Australian Auditing Standards Board, Parkes currently serves as chairman or independent member of a number of audit committees in Australia.
Outsourced Activities

5. Outsourced information management and storage (all value stored, databases, customer files, key parameters, etc.)

Risks From Outsourcing and Possible Consequences

Very high risk—Depending on how critical the information stored with the outsourcer is (and does the outsourcer understand this)

- Loss of information through penetration, hacking
- Data corruption or inability to provide service
- Risks of embarrassment to reputation in the marketplace
- Breach of contract/risks of legal action
- Costs of recovery

IT Governance Considerations for Executives and Boards

- Ensure the outsourcing contract covers customer access and clear responsibilities for ownership of information.
- Profitability of service and cost of the level of service actually provided
- Ensure adequate backup and disaster recovery arrangements have been made. Executives should cite specific evidence of successful recovery testing. Directors should request written confirmation from CEO that this testing has been confirmed as taking place.
- Inquire as to security over information stored for customers.
- Inquire as to information management effectiveness, e.g., is it reliable, is the customer advised of quality issues on data received?
<table>
<thead>
<tr>
<th>Outsourced Activities</th>
<th>Risks From Outsourcing and Possible Consequences</th>
<th>IT Governance Considerations for Executives and Boards</th>
</tr>
</thead>
</table>
| 4. Outsourced core knowledge systems and development of new or maintenance of existing systems (e.g., corporate memory, key knowledge elements, activity processes, executive preferences) | High to very high risk—Depending on how critical the outsourced knowledge systems are to the customer  
- Keeping customer’s systems operating at agreed uptime and service levels  
- Continuing ability to develop new systems and associated intellectual property  
- Continuing ability to maintain/support customer’s existing software in times of rapid change or where there are major redesign/paradigm changes to install  
- Loss of software skills, especially on obsolete software languages still requiring support | • Ensure adequate backup and disaster recovery arrangements have been made (as noted).  
• Inquire deeply as to security over systems stored at the data centre on behalf of customers.  
• Inquire deep into the security of associated communication channels.  
• Ensure contracted software development and software maintenance services are provided to contracted standards.  
• Inquire deeply as to project delivery management for new systems.  
• As to system uptime and maintenance performance, e.g., are service delivery levels being consistently met?  
• Ensure that the recruitment and training of staff with required skills is taking place. |
| 3. Outsourced major computer installation and ancillary support services              | Medium to high risk  
- Cost of keeping major data centres operational and able to provide contracted support services  
- Cost of investment in future technology infrastructure to remain market-credible, competitive and sustainable  
- Changing ways of doing business may lead to customer paradigm shifts. | • Ensure adequate backup and disaster recovery arrangements have been made and tested (as noted).  
• Limit disruption caused by auditors providing assurance reports on installation service and uptime performance; consider appointing a sole provider for this purpose.  
• Ask if the contracted service and uptime operational commitments are being met by the data centre.  
• Ensure customers are not being overserviced or are paying for services out of the agreed scope. |
| 2. Outsourced networks or communications                                            | Medium to high risk  
- Risks include illegal or malicious penetration (hacking), denial-of-service attacks, information or system corruption, intellectual property theft, viruses, worms and Trojan horse attacks.  
- It is critical to provide alternate network routing where outsourcer also provides networking services to customer.  
- Insufficient communications capacity to meet customer demands/contracted service levels. | • Ensure that adequate backup and disaster recovery arrangements have been made and tested (as noted).  
• Inquire as to security at all points of the network, extranets and intranets, as well as over links to the Internet, Internet service providers (ISPs), Internet service and web sites directly linked to the data centre.  
• Ensure that adequate capacity planning is done to meet expected customer demand trends. |
| 1. Provision of computer equipment, replacement of network PCs and servers, network devices | Usually low risk  
- Market competition  
- Contract not meeting customers’ needs over time  
- Excessive service demands from customer | • Comply with terms of outsourcing agreement (service provided/payments received).  
• Ask about the condition of customer relationship and customer satisfaction levels with outsourced IT services provided. |