



AMPER, POLITZINER & MATTIA, P.C.
CERTIFIED PUBLIC ACCOUNTANTS
and CONSULTANTS

North Jersey Chapter

Institute of Internal Auditors

What Internal Audit Needs to Know About The
Risks of Outsourcing and Role of SAS 70
Reports

January 17, 2008



AMPER, POLITZINER & MATTIA
CERTIFIED PUBLIC ACCOUNTANTS
and CONSULTANTS



Risks of Outsourcing Key Business Processes to Third Party Vendors



AMPER, POLITZINER & MATTIA
CERTIFIED PUBLIC ACCOUNTANTS
and CONSULTANTS



Basic Premise

Although certain risks and control activities may have shifted to the outsource provider, Senior Management still maintains the responsibility to understand and periodically review the outsource environment. In the end, responsibility for achieving control objectives still rests with Management.



Overview

Outsourcing key business processes to third parties is now common practice for many organizations.

Initially, outsourcing was viewed simply as a way to reduce costs; over time, outsourcing has helped organizations achieve significant business value.

However, a constant challenge for any organization is how well they deal with the resulting risks from outsourcing a key business process.

Risks need to be considered within the environments of both the User and Service Provider

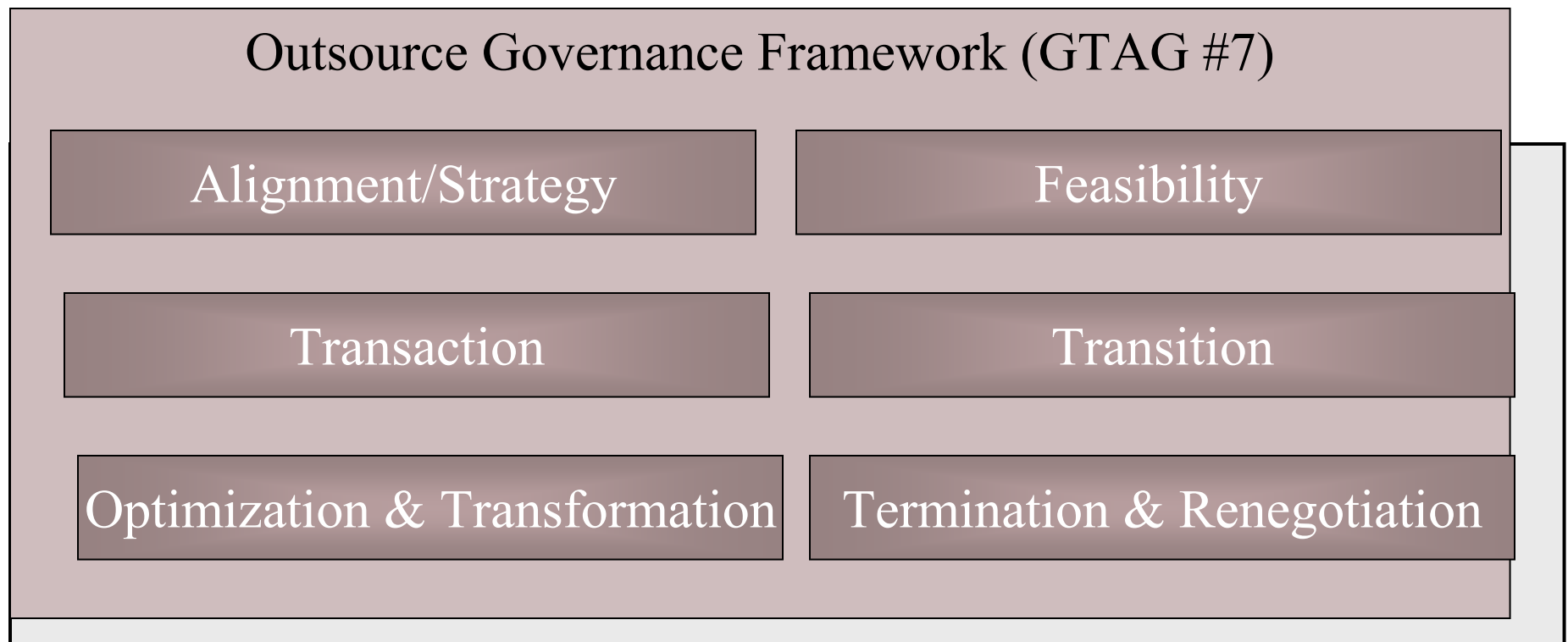


Risk Considerations within the User Environment

Risks present themselves before an outsourcing relationship is initiated and throughout its lifecycle. Regardless of the business function being outsourced, an organization should have a well developed business case which specifies the cost/benefit aspects for the relationship.



Risk Considerations within the User Environment





RISKS	IMPACT
<p>Strategy: Outsourcing strategy is not aligned with corporate objectives</p>	<ul style="list-style-type: none"> •The decision to outsource is the wrong one •The contract is not set up and managed in line with corporate objectives
<p>Feasibility: Assumptions (Payback period, cost savings) are wrong as the result of inadequate due diligence and failure to assess relevant risks</p>	<ul style="list-style-type: none"> •The potential for outsourcing is not explored in detail, resulting in the lack of fully derived benefits •The contract is awarded to an inappropriate provider •Issues are not managed efficiently and effectively because they were not anticipated
<p>Transaction: Procurement policies are not met; proper contracts (service level agreements) are not implemented; operational, HR, and regulatory implications are not considered and contingency arrangements are not made</p>	<ul style="list-style-type: none"> •Absence of a well drafted agreement could lead to a situation in which the organization might be unable to rely on a legally binding document to ensure compliance for intended contractual terms •Potential breaches of regulatory compliance exist that lead to financial penalties and negative press
<p>Transition: There is a lack of formal transition planning, failure to plan for retention of appropriate skills</p>	<ul style="list-style-type: none"> •Loss of key resources during the transition period •Loss of confidence in the outsource service •Operational difficulties
<p>Optimization & Transformation: The outsourcing contract is not managed effectively. Outsourcing benefits and efficiencies not achieved</p>	<ul style="list-style-type: none"> •The ROI is not what was expected or is minimal compared to costs •Services are below expectation levels •Rise of unplanned costs
<p>Termination & Renegotiation: There is an inadequate termination of outsourcing processes</p>	<ul style="list-style-type: none"> •The organization is unable to take over the outsourced activity at a later date or issues in terminating or renegotiating the contract



Risk Considerations within the Service Provider's Environment

When outsourcing a business process, keep in mind that some of the controls previously at the user organization transfer totally or in part to the service provider. In such cases, consideration of risks need to expand beyond the user environment.



RISKS	IMPACT
<p>Control Environment: Poor control environment may be a sign for control issues and ability to provide quality service.</p>	<ul style="list-style-type: none"> • Poor service levels • Inability to meet terms and conditions of the contract
<p>Security Considerations (including data, network, physical, personal and logical access) : Data is lost or compromised resulting in an ability to serve and/or negative press</p>	<ul style="list-style-type: none"> • ROI may not be achieved due to an inefficient process • Loss of sensitive organizational data • Service provider down-time due to security breach affecting ability to efficiently provide service
<p>Business Continuity: Lack of a plan may inhibit the availability of the service provider to continue to provide service</p>	<ul style="list-style-type: none"> • Service levels will be compromised in the event of a disaster or disruption at the service provider • Loss of organizational confidence • Lack of response time
<p>SDLC & Integration: There are no formal processes, policies & procedures to ensure that controls are in place over the system, data or transactions administered by the service provider</p>	<ul style="list-style-type: none"> • Organization may face control or data integrity issues when incorporating the results from a service provider into its own environment
<p>Change Management & Update Procedures: Processes are not updated to reflect process improvements, accounting or regulatory changes</p>	<ul style="list-style-type: none"> • Organization may face control or data integrity issues when incorporating the results from a service provider into its own environment • Organization may be non-compliant with certain regulatory or accounting matters
<p>HR Policies & Procedures: Policies and procedures are not consistent with the User Organizations policies</p>	<ul style="list-style-type: none"> • Possible ethical issues; questionable business practices • Employee incentives are unrealistic and may impact performance • Inadequate employee resources affecting service



Impact of Outsource Risks on the Internal Audit Plan and Internal Audit Considerations



AMPER, POLITZINER & MATTIA
CERTIFIED PUBLIC ACCOUNTANTS
and CONSULTANTS



Overview

Remember that when outsourcing a business process, some of the controls previously embedded within the user organization transfer totally or in part to the service provider. As a result, an internal auditors scope needs to extend beyond the user organization into that of the service provider.

When performing their risk assessment and creating their audit plan, internal auditors should work with the organization to identify all outsource relationships

Pending on the risk, an evaluation of the outsource provider and related user controls should be included in the audit plan

Keep in mind that the procedures performed by Internal Audit may be affected if the outsource agreement does not contain a Right to Audit provision.



Internal Audit Considerations

Nature, Extent and Timing of Internal Audits

- The nature of the procedures performed at the service provider may range from:
 - Reading and reviewing a SAS 70 report (if one exists),
 - Performing a walk through on certain classes of transactions or certain key processes,
 - Full-scope internal audit engagement.
- The extent of the procedures must be sufficient to determine that the control objectives have been sufficiently satisfied to cover all relevant risks.
- Controls must be evaluated at both the outsource provider and the organization; the level and sufficiency of the organization's controls will influence the amount of effort and extent of testing at a service provider
- Understanding whether or not the service provider has modified its controls to satisfy their relationship with the organization will also impact audit procedures
- If a service auditor's report is available, the date and time period covered should be considered in determining whether or not additional procedures need to be performed; this is of particular importance when evaluating the controls of an outsourced business process for Sarbanes-Oxley requirements.



Areas of Focus for Internal Auditors

- Assess the adequacy of the User controls:
 - Usually this assessment may be made via the performance of a walkthrough
 - Evaluate the detective/monitoring controls deployed by the organization; examples include:
 - Transactional reviews to identify errors that are more than inconsequential
 - Reperforming significant calculations for reasonableness
 - Financial Statement Reviews
 - Budget to Actual Variances
 - Identification of process changes; for instance, new regulations or accounting pronouncement
 - Review the process and procedures for how the user monitors and manages the outsource relationship from beginning to end
 - Have communication channels been clearly established
 - Definition of roles and responsibilities and statement of work
 - Adequacy of the business case and assumptions used in the business case
 - Vendor selection process
 - Bidding process
 - Service providers capabilities and ability to execute all aspects of the agreement
 - Contract Review (terms and conditions)
 - Contract compliance/penalties
 - Transition/Sustainment plans; Knowledge transfer
 - Change order and renewal process



QUESTIONS?



AMPER, POLITZINER & MATTIA
CERTIFIED PUBLIC ACCOUNTANTS
and CONSULTANTS