Practical Guide for IT Outsourcing

Version 3.0

Table of Contents

Outsourcing Management Standard

Overview

Outsourcing does not remove the enterprise's requirement to manage the process. A comprehensive outsourcing arrangement requires Service Level Agreement (SLA) monitoring and redefinition, as well as strategic management and other retained functions. (See outsourcing approval standard under retained costs – Page 11 for a listing of frequently retained functions).

As you start an Outsourcing Process there are many factors to consider before you past a point of no return. Examples of these are:

- ✓ If your enterprise is going through periods of rapid or dramatic change, including changes in the way you do business, how will outsourcing impact this?
- ✓ Your enterprise's IT function is efficient and has a low cost of operation, what value will the outsourcer provide?
- ✓ The primary motivator for outsourcing is the drive to reduce costs, why could you not do the same internally?
- ✓ The enterprise does not have the management talent or competency to plan and manage the outsourcing process and outsource provider, how will you know that you are getting value from your outsourcer?
- ✓ Outsourcing is being driven by senior management that does not have a strategic vision of where the enterprise is going, is the driver behind this move someone who thinks this is the "in" thing to do?
- ✓ Internal costs of the IT function are not fully understood, how will you know that you are getting the most cost effective solution from your outsourcer?
- ✓ Performance metrics are not well defined for the IT function, how do you know that the service provided by your outsourcer will be as good if not better than what the enterprise is getting today?
- ✓ The enterprise operations are entwined with IT functions such that if the IT function is outsourced a significant amount of core enterprise functionality and operational knowledge will have to be transferred to the outsourcer, will the outsourcer have a large "learning curve"?
- ✓ The enterprise's strategic plan has not been defined with all of the outsourcing im of th

Standard

Service Level Agreements (SLA)

The Service Level Agreement (SLA) is the central instrument for managing an outsourced function (See page 48 for sample SLA). The Manager of Outsourcing (see page 44) will track SLA (See Service Level Agreement Report Package section – page 16) fulfillment and enforce the contract terms if an SLA is not met. The Manager of Outsourcing must also take an active role in defining and redefining SLAs in order to take into account changes in the operating environment. [1]

Problem Responsibility

The efficient assignment of end-user complaints to the appropriate entity is critical to maintaining high service-levels. IT will ensure that the all staff is trained in order to identify whether a problem lies with IT or a particular vendor[2]. In a multi-vendor environment this task becomes even more critical, if one is to avoid a constant reassignment of problems.

The Manger Outsourcing or a role similar to that should perform this function.

Outsourcing Policy Standard

Policy Statement

The enterprise's business units will consider the outsourcing of parts of its Information Technology (IT) function if such an arrangement could provide savings and true added value. Outsourcing decisions will not be made without a formal "base case" analysis that demonstrates the cost-effectiveness of the outsourcing decision. Outsourcing contracts will be finite and will hold the Vendor to a Service Level Agreement (SLA). SLAs will contain clear penalties associated with failure to meet minimum service levels.

Goal

The goal of outsourcing is to seek areas in which a vendor's economies of scale are able to streamline IT's operations, add value, and allow the enterprise to concentrate its efforts on core competencies.

[1] ***Additional information and examples can be found at http://www.e-janco.com/ in the Internet and Information Technology Metrics HandiGuide®.***

[2] ***Each vendor must sign a non-disclosure agreement see sample agreement***

Outsourcing Approval Standard

Overview

The decision to outsource a segment of the IT function is a complex and ongoing process that requires a good deal of expertise in its own right. Approval of an outsourcing agreement requires the implementation of Service Level Agreements, an initial analysis of outsourcing scope, base case analysis, vendor identification, request for price quote, vendor bid appraisal, and contract negotiation. Each of these steps must be performed successfully in order to achieve a positive outsourcing decision.

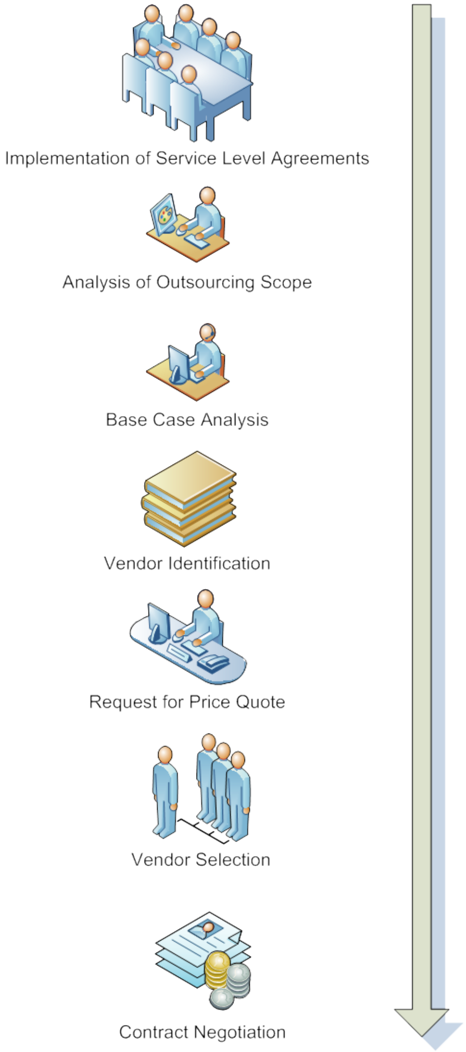

Figure 1 Outsourcing Process Chart

Standard

The decision to seek an outsourcing solution must be evaluated carefully by IT so that all appropriate considerations are made prior to entering into a contractual relationship. An enterprise will consider outsourcing as an option for parts of its IT function under the following circumstances:

- Outsourcing the function will allow greater focus on a business unit's core competencies, while freeing management, at least in part, from distracting day-to-day IT functions;
- A field is so dynamic, that keeping up has become a significant drain on IT's resources; or
- The economies of scale provided by the vendor will produce significant cost savings for the enterprise.

Prior to initiating a Request for Proposal (RFP), a "base case" analysis should be completed.

Base Case

A base case (see base case development page 42 for items to consider) is a low-level analysis of the expenses associated with the operations being considered for outsourcing. Once completed, a base case will become a precise estimate of the predicted "in-house" costs of running the function being considered for outsourcing over the target time-span.

While a base case does not address the non-financial aspects of the outsourcing decision, it is indispensable for establishing the extent of expected savings that may be achieved. It is also the baseline that will be used when comparing competing bids.

Risk Assessment

Management shall nominate a suitable owner for each business function/process outsourced. The owner, with help from the local Information Risk Management Team, shall assess the risks before the function/process is outsourced, using ENTERPRISE's standard risk assessment processes.

In relation to outsourcing, specifically, the risk assessment shall take due account of the:

- ✓ Nature of logical and physical access to ENTERPRISE information assets and facilities required by the outsourcer to fulfill the contract;
- ✓ Sensitivity, volume and value of any information assets involved;
- ✓ Commercial risks such as the possibility of the outsourcer's business failing completely, or of them failing to meet agreed service levels or providing services to ENTERPRISE's competitors where this might create conflicts of interest; *and*
- ✓ Security and commercial controls known to be currently employed by ENTERPRISE and/or by the outsourcer.
- ✓ The result of the risk assessment shall be presented to management for approval prior to signing the outsourcing contract. Management shall decide if ENTERPRISE will benefit overall by outsourcing the function to the outsourcer, taking into account both the commercial and information security aspects. If the risks involved are high and the commercial benefits are marginal (*e.g.* if the

Financial

Report	Metrics
Key Measures	All data is captured for a rolling 13 months Expenses - Period Actual (Dollars) Expenses - Period Plan (Dollars) Staffing - Period Actual (FTEs[21] Staffing - Period Plan (FTEs) On-line Availability[22] - Plan (%) On-line Availability - Actual (%) Billing Performance - Plan (Dollars) Billing Performance - Actual (Dollars)
Expense Performance Summary	All data is captured for a rolling 13 months Current Period - Actual (Dollars) Current Period - Plan (Dollars) Year to Date - Actual (Dollars) Year to Date - Plan (Dollars) YTD Variance from Plan - Period (Dollars) YTD Variance from Plan - YTD (Dollars)
Expense Variance by Category	All data is captured for current fiscal year by budget category Current Period - Plan (Dollars)
Expe	er Cumulative YTD - Plan (Dollars) Cumulative YTD- Actual (Dollars) Cumulative YTD - Actual (Variance Analysis)

Financial Metrics - Part 1 of 2

[21] *FTE is Full Time Equivalents)*

[22] *Some users prefer man hours or revenue lost due to failure of system availability. This is a negative measure and we have opted to show only positive metrics in this set of metrics.*

ISO 27001 & 27002 - Security Process Audit Checklist

NOTE: If you implement the Janco Security Manual Template completely you will meet all of the points listed on this Checklist.

Security Policy Management Objectives

Establish a comprehensive information security policy:

- Validate that your enterprise's information security policy provides clear direction for your enterprise's information security program.
- Validate that your enterprise's information security policy shows that your management is committed to information security.
- Validate that your enterprise's management supports your enterprise's information security policy.
- Validate that your enterprise's information security policy shows that your management is prepared to support an ongoing commitment to information security.
- Validate that your enterprise's information security policy is consistent with your business objectives.
- Validate that your enterprise's information security policy meets your enterprise's business requirements.
- Validate that your enterprise's information security policy complies with all relevant laws and regulations.

Corporate Security Management Objectives

Establish an internal security organization.

- Establish a management framework to control how your enterprise implements information security.
- Validate tha olicy.
- Validate tha
- Validate tha s your enterprise.
- Validate tha ur enterprise.
- Validate tha ur own enterprise.
- Validate that your enterprise's internal experts are able to provide specialized information security advice.
- Validate that your enterprise has access to external security experts, advisors, and authorities.
- Use your external advisors to help your enterprise monitor changes in security standards.
- Use your external advisors to help your enterprise monitor changes in security assessment methods.
- Use your external advisors to help your enterprise keep up with industrial security trends.
- Validate that your enterprise's external information security experts and advisors can help your enterprise to deal with security incidents.
- Validate that your enterprise's enterprise encourages the use of a multi disciplinary approach to information security.

Control external use of your enterprise's information.

- Maintain the security of your enterprise's information whenever it is being accessed by external parties.
- Maintain the security of your enterprise's information whenever it is being processed by external parties.
- Maintain the security of your enterprise's information whenever it is being managed by external parties.

Risk Assessment Business & IT Impact Questionnaire

Version 4.0

Table of Contents[1]

[1] Sections of this document were extracted from Disaster Recovery Template, Client Server Management HandiGuide, PC Policies and Procedures HandiGuide, Metric for the Internet and IT Management HandiGuide, and the IT Position Description HandiGuide which are copyrighted by M. V. Janulaitis and published by Janco Associates, Inc. These copyrighted materials remain the property of the copyright owners and the licensed user of this document is only granted a limited use license of this material. For more information, see http://www.e-janco.com

ENTERPRISE
Business and IT Impact Questionnaire

The purpose of this questionnaire is to determine the criticality of the applications used at ENTERPRISE. The information provided will be used to develop a Application Inventory that can be used in the Disaster Recovery Plan that minimizes the impact of the loss of this application in the event of a disaster. **(PLEASE USE ADDITIONAL BLANK PAPER OR ATTACHMENTS WHEREVER NECESSARY)**

Facility / Business Function / Application

Name: ______________________________

Provide a brief description/purpose – mission: ______________________________

____

____

What are the main functions? ______________________________

____

____

____

____

____

Was this developed in-house or purchased from a vendor? If purchased from a vendor, do you hold the plans, source code etc: ______________________________

____

If the application is ication (briefly describe modifications): ______________________________

____

____

What programming language was used to create the application? ______________________________

____

How old is this application (maturity)? ______________________________

Who is the owner of this application (i.e. Joe Smith of Accounting)? ______________________________

____

Preparer: ______________________________ Date: ____________________

User Environment

Provide the following information for each department that uses the application:

- Department name
- How the application is used (example: Department A inputs patient information, Department B enters billing information etc.)
- Primary contact (i.e. primary user or department head name)
- Number of people in department that use the application
- What attribute best describes the users that have access to this application:
  - Public
  - Customers and Employees
  - Groups of Employees
  - Specific Employees
  - Other __________

Department Name	Purpose or Use	Primary Contact	Number of Users	User Attribute
				□ Public □ Customers □ Employees □ Groups of Employees □ Specific Employees □ ____________
				□ Public □ Customers □ Employees □ Groups of Employees pecific Employees ____________
				ublic ustomers mployees roups of Employees pecific Employees ____________
				ublic ustomers mployees □ Groups of Employees □ Specific Employees □ ____________
				□ Public □ Customers □ Employees □ Groups of Employees □ Specific Employees □ ____________
				□ Public □ Customers □ Employees □ Groups of Employees □ Specific Employees □ ____________
				□ Public □ Customers □ Employees □ Groups of Employees □ Specific Employees □ ____________

Preparer: ______________________________ Date: ________________

Criticality of Application

Are there any particular aspects of this system's operation or function that should be considered in determining the system's criticality to the organization? ____

____

____

____

If a disaster occurred and normal processing capability were unavailable, in which of the following categories would you classify this system:

Category I □ Must be processed in normal mode, no degradation is acceptable.

Category II □ Only high priority (i.e., high dollar item) transactions or critical reports would be processed.

Category III □ Processed would be carried out on a "Time Availability" only basis.

Category IV □ Processing would be suspended, but data collection would continue.

Category V □ No pr

How long can application be n?

□ 0

□ 3 - 5 Days □ 5 - 10 Days □ Greater Than 10 Days

What would be the first major affect if system were to go down (i.e. Patients would not receive medicine?

____

____

____

How long until the next impact (i.e. monthly processing could not be performed)?

____

____

____

____

Preparer: ______________________________ Date: ____________________

ENTERPRISE
Business and IT Impact Questionnaire

Application / File Servers Continued

Host Name: ____________________________	**Reviewer Name:** ___________________________________	**Date:** ___________________

IP Address / Mask	**User Types**	**Administrative Contact**	**Connectivity**	**Physical Location**
___.___.___.___ ___.___.___.___ **(mask)**	□ Public □ Customers □ Employees □ Groups Employees □ Specific Employees □ _______________	Name: _______________________ Email: _______________________ Phone: ______________________	□ Internet □ Intranet □ Modem In Bound □ Modem Out Bound □ Other: ____________	Address: __________________ Contact::__________________ Phone: ___________________
IP Address Range	**Operating System**	**Version / Reviewed**	**Application**	**Version / Reviewed**
___.___.___.___ to ___.___.___.___	□ Windows WS □ Windows Server □ Unix □ Lynx. □ Other ________	Ver: ____________ □ Yes □ No Ver: ____________ □ Yes □ No Ver: ____________ □ Yes □ No Ver: ____________ □ Yes □ No	□ _________________ □ _________________ □ _________________ □ _________________	Ver:__________ □ Yes □ No Ver:__________ □ Yes □ No Ver:__________ □ Yes □ No Ver:__________ □ Yes □ No ________ □ Yes □ No ________ □ Yes □ No

Comments: ____

____

____

____

____

____

____

____

____

Preparer: ______________________________ Date: ________________

What's New

Version 4.0 – February 2010

- ❑ Updated for COBIT compliance
- ❑ Updated for PCI-DSS compliance
- ❑ Updated for US state level compliance (New York, Massachusetts, and California)\
- ❑ Update for ISO security requirements

Version 3.3 – February 2008

- ❑ Updated to be ISO 27000 Series compliance
- ❑ Correct minor errata
- ❑ Updated formatting

Version 3.2 – February 2007

- ❑ Updated to meet ISO 17799 compliance standard
- ❑ Application / File Servers form was added
- ❑ Operating Environment was moved forward in the forms
- ❑ Critically of Application was moved forward in the forms

Preparer: ______________________________ Date: ________________

What's new

Version 2.4 – February

- Updated Risk Assessment – Business and IT Impact Questionnaire
  - ✓ Updated for COBIT compliance
  - ✓ Updated for PCI-DSS compliance
  - ✓ Updated for US state level compliance (New York, Massachusetts, and California)\
  - ✓ Update for ISO security requirements
- Updated Outsourcing Policy
- Added Outsource Security Policy Compliance Agreement

Version 2.3 – November 2008

- *Updated to use WORD CSS style sheet*
- Update Business and IT Impact Questionnaire –in addition to being included as part of the main document it is included as a separate PDF and Word document.

Version 2.2 – February 2008

- Updated text to conform to Sarbanes-Oxley
- Updated contract terms to include staffing approval requirements
- Added section of criteria for selecting vendor candidates
- Updated ISO Security Audit Checklist to meet ISO 27001 and ISO 27002
- Updated graphics

Version 2.1 – February 2007

- Updated text to conform to Sarbanes-Oxley
- Added updated Business and IT Impact Questionnaire
- Added ISO 17799 Security Audit Checklist
- Added Outsource Security Policy Compliance Agreement
- Added HIPAA Audit Program Guide
- Updated selected graphics
- Corrected minor errata