Trustworthy Computing

Spring 2006

Project Topic:

Risk Management of Information Technology Outsourcing

under ITIL ITSM framework

By: (Mina) Szu-Chia Cheng

Table of Content

Abstract

This report covered the Business Risk Management and Information Trust and Compliance issues which discussed management process of identifying, measuring, monitoring, and controlling the risks associated in outsourcing information technology scenario. The major focus of this paper is to describe the monitoring process which setup up by ITIL ITSM framework.

The content of this project includes the introduction about IT outsourcing risks, concept of ITIL and ITSM, and ITSM framework. For case study part is discussed the HP ITSM, which dicussed the how ITIL influence ITSM, ITSM components, and discessed P&G ITSM experience in IT outsourcing control tool, which told us that the ability of ITIL ITSM could manage IT process effectively, and get more control power after outsourcing the IT operation.

Why business should care IT outsourcing risk?

Outsourcing non-core activities has been a major trend over the last decade, starting with the IT function, where specialist companies are able to take over an enterprise's entire data centre operation. But the market has grown and evolved tremendously, to encompass a whole range of business processes.

In the past, IT outsourcing involved the typical data centre operation, where huge computers fed by a host of peripherals processed large volumes of numbers that were printed out or stored on some form of magnetic storage device and then delivered to the client. These were essentially number crunching warehouses that didn't delve too deeply into the business that the numbers represented.

With the growing trend toward focusing on core business capabilities, many companies are outsourcing selected business functions to expert partners who can perform them more efficiently and cost-effectively. The security management of IT outsourcing now became a serious subject for business, since managing all types of risk is the key of building a successful business. Understanding risk allows organizations to properly manage resources towards areas that are risk averse and make decisions that add or reduce risk. Moreover, IT needs are should always be driven by organizational needs, therefore, we could say: IT risk is driven by organizational risks. Hence, it is important to understand IT risk in the context of business risk because the operations, compliance and financial well-being of an organization will drive risk to IT.

Ultimately, outsourcing, regardless of the activity, is a business decision rather than a technology issue.

IT Outsourcing risk evaluation and control

An outsourcing risk assessment should consider the following:

- Strategic goals, objectives, and business needs of the financial institution.

- Ability to evaluate and oversee outsourcing relationships.

- Importance and criticality of the services to the financial institution.

- Defined requirements for the outsourced activity.

- Necessary controls and reporting processes.

- Contractual obligations and requirements for the service provider.

- Contingency plans, including availability of alternative service providers, costs and resources required to switch service providers.

- Ongoing assessment of outsourcing arrangements to evaluate consistency with strategic objectives and service provider performance.

- Regulatory requirements and guidance for the business lines affected and technologies used.

ITIL and Outsourced Services

It could be argued that the fact that a function is delivered externally requires even more stringent and disciplined management structures than internal delivery. Certainly, there are a significant number of aspects that require close attention and for which the application of ITIL disciplines can bring substantial benefits.

The application of ITIL is actually core in many of these areas. The different ITIL issues still need to be tackled, perhaps through slightly different methods: Problem Management, Change

Management, Service Level Management, Continuity Management, etc.

Certain ITIL disciplines will emerge as fundamental, such as Service Level Management. Others will be employed more actively during the outsourcing transition. However, the use of ITIL will certainly help ensure a more rigorous and robust arrangement, which ultimately should benefit both parties.

Key Techniques, Components, and Models

ITIL Overview

What is ITIL?

ITIL is best practice in IT Service Management, developed by OGC and supported by publications, qualifications and an international user group. ITIL is intended to assist organizations to develop a framework for IT Service Management. Worldwide, ITIL is the most widely used best practice for IT Service Management. ITIL also provides process support to help ensure that the financial records and data of public-traded corporations are managed in full compliance with the Sarbanes-Oxley Act (SOX).

What are the benefits of using ITIL?

ITIL provides a systematic and professional approach to the management of IT service provision. Adopting its guidance can provide such benefits as:

■   reduced costs

- improved IT services through the use of proven best practice processes

- improved customer satisfaction through a more professional approach to service delivery

- standards and guidance

- improved productivity

- improved use of skills and experience

- improved delivery of third party services through the specification of ITIL or BS15000 as the standard for service delivery in services procurements.

ITSM Overview

What is meant by 'IT Service Management'?

IT Service Management is a set of processes that cooperate to ensure the quality of live IT services. IT Service Management provides an overall framework within which to operate individual activities such as the Service Desk and the implementation of Service Level Agreements (SLAs).

The principal objectives of IT Service Management are:

- providing customer focussed IT Services

- aligning IT services with the organisation's objectives

- the implementation and management of cost-effective SLAs

IT Service Management is based on best practice documented in the IT Infrastructure Library (ITIL), which was the outcome of a major UK Government funded project embracing public and private IT service providers. The ITIL is the basis of BS15000 and AS8018, the UK and Australian standards for IT service management best practice.

IT Service Management can help:

- Turn your technology focused group into one with a service focus.

- Ensure IT services are aligned with, and satisfy business needs.

- Improve system reliability and availability.

- Provide a basis to agree levels of service and the ability to measure IT service quality.

The benefits of implementing ITIL are many the most beneficial include:

- Aligning IT with business needs

- Move from a technology to a service based culture

- More ability to absorb rapid change

- Improve the quality of IT Services

- IT perceived as offering value to the organization

- Ensure everyone speaks the same language.

Over a period of time, a successful ITIL implementation should show improvements in:

- the availability of IT services

- customer satisfaction and the reputation of the IT operation and

- effectiveness of the IT operation, and the opportunity to move staff from firefighting activities to planning activities.

Case Discussion - HP IT Service Management (ITSM)

Why HP uses ITIL in IT standard process development?

First, while it is understood that the ITIL books clearly address "process," they do so at a very high level, fulfilling the role as "conceptual" guides for understanding "what" processes are required by IT and "what" those processes should do. They don't tell you "how" to do anything! No one can pick up an ITIL book and implement a process.   To do this requires two things - more in-depth knowledge about the process and knowledge about "how" to do process design, implementation and management - none of which is provided by ITIL.   To address these issues, HPC [1] incorporated industry standard process management techniques and process design methodologies into its ITSM service offerings and began building a set of ITSM collateral based on real-world implementation experience.

Second, although the ITIL books address process-specific roles and responsibilities, these are again, very high level and ITIL doesn't offer much to people faced with the painful task of changing the way they do things. To address this, HPC created more detailed roles and responsibilities and incorporated "management of change" concepts and techniques into their IT Service Management offerings to ensure easier transitions for the people affected by process implementation.

Third, the ITIL books were written to help companies who wanted to run IT "within" a business, whereas the later the industry believed that IT organizations needed more – they needed to know how to run IT "as a business," which meant that the processes offered by ITIL were incomplete. To address this, HPC identified and defined several new IT processes not covered by

---

[1] HPC = Hewlett-Packard Consulting

ITIL, processes that are critical to running IT "as a business."

Lastly, the ITIL processes were originally defined in the 1980's and weren't really changed much until 2002, which means that they were very mainframe-centric. To implement these ITIL processes in today's distributed environment meant some things in ITIL were fine as is; others had to be changed, while still other processes did not apply at all.

HP IT Service Management (ITSM)

In the early 1990's, HPC began an IT Service Management effort to develop solutions for customers based on ITIL. HPC defined IT Service Management as *"A business-driven approach to reengineering IT, focused on delivering IT services to business customers at agreed-upon service quality and cost targets."* It quickly became apparent however, that "complete" ITSM solutions for customers required more than ITIL had to offer.

Components of HP ITSM

1. Helpdesk / Incident Management

2. Problem Management

3. Change Management

4. Software Control & Distribution

5. Configuration Management

6. Service Level Management

7. Cost Management

8. Capacity Management

9. Availability Management

10. Contingency Planning

How the HP ITSM Reference Model integrates with the COBIT framework

Understanding the control framework: COSO and COBIT

Are there too many IT-related "surprises" that impact business objectives? Are IT service levels for important business processes monitored effectively? Do good internal communication and reporting about control exist? Does IT provide service level metric visibility to the line of business managers? Does IT have issues about providing visibility? These are just some of the questions companies are being forced to ask when contemplating their Sarbanes-Oxley compliance. At its most fundamental, the Sarbanes-Oxley Act is about control and documented accountability Implementing the COSO and COBIT frameworks of control helps companies do both.

The Committee of Sponsoring Organizations of the Tread way Commission Internal Control Framework (COSO)

COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through corporate governance, effective internal controls and business ethics. The entire accounting industry recognizes and embraces the COSO internal controls framework. COSO provides a standard against which businesses can assess their control systems and determine how to improve them.

Control Objectives for Information and related Technology (COBIT)

A widely accepted reference tool for IT control, COBIT is an authoritative framework used by management, IT professionals and internal and external auditors. Now in its third edition, COBIT is published jointly by the IT Governance Institute and The Information Systems Audit

and Control Association.

COBIT is a set of good practices that provides a standard against which companies can assess their IT control systems and determine how to improve them. COBIT defines 34 IT control objectives that fall into four categories:

1. IT planning and organization control objectives

2. IT acquisition and implementation control objectives

3. IT delivery and support control objectives

4. IT monitoring control objectives

When applied to COSO and COBIT, the HP ITSM Reference Model gives companies real solutions for a tightly-controlled system.   Each COSO component is controlled by each of the COBIT objectives. Similarly, each of the COBIT objectives maps to a correlating business process. That's where the HP ITSM Reference Model comes in.

Here's how it works:

■   COBIT's Planning and Organize maps to the ITSM Reference Model's Business-IT Alignment

■   Acquire and Implement maps to both Service Design & Management and Service Development & Deployment

■   Deliver and Support maps to Service Operations

■   Monitor and Evaluate maps to Service Delivery Assurance

See detail mapping chart in appendix 1.

The HP ITSM Reference Model

IT Service Management (ITSM) manages the quality and quantity of delivered IT services. It is an approach to delivering business-critical IT services that focus on meeting cost and performance targets set in partnership with internal customers and embodied in service agreements. Service management is a layer of management capability that the IT organization must build to cope with today's IT environment and improve its relationship with the business. The service management layer sits above the networked system management layer and bridges the gap between business management and the technical management of specific networked information systems and their component elements (see figure below).
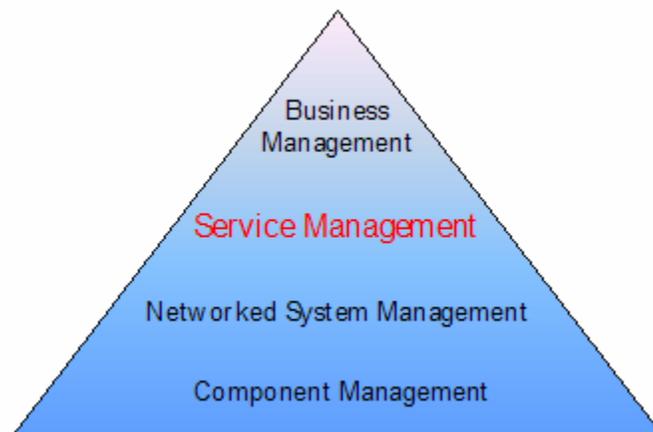
Today, the emphasis on "customer-focus" within IT is becoming pervasive, and reflects the demand from IT customers that IT must become a valued business partner – or be replaced. Some of the key transitions IT organizations are facing:

- Stop viewing the consumers of their services as "users," and start viewing them as "customers"

- Temper their traditional "inward" perspective and start looking "outward"

- Expand their focus on technology to include a focus on process

- Move away from isolated "ad hoc" processes and start developing business-justified, streamlined IT processes

- Stop attempting to address customer service requirements with "best effort" process improvements and start implementing "measured, accountable" IT processes

- Expand their work efforts, which have historically been centered on "in house" solution developments, to include a cost-justified balance between "internal-sources" and "outsourcing"

- Develop and implement integrated, end-to-end IT processes and discard those processes that are fragmented, therefore avoiding process "silos"

- Use the new process improvements to change the reactive IT organization to one that is proactive

- Define and develop new service-oriented roles and responsibilities

- Embellish the traditional IT "system" skills with new customer-focused skills, by learning to "listen" to the customer

The HP ITSM Reference Model is NOT intended to depict an ideal organizational structure but is designed to capture and show the integration of 16 key IT processes. A diagram of the model is shown in appendix 2.

How HP ITSM helps P&G control the IT outsourcing?

Procter & Gamble implemented ITIL in order to make its operations more efficient and reduce costs.

According to Procter & Gamble, operating expenses are continually being reduced in the range of 15-20% per year, with $500 millions having been removed from the expense pool. From a

practical standpoint, Procter & Gamble used standardization of process to implement 'follow the sun' support, where support moves from one support center to another so that 24x7 support is delivered according to a rotating series of day shifts in different time zones. ITIL provides the necessary standardization of procedures between groups.[2]

In 2003 August, Hewlett-Packard announced a $3 billion, 10-year agreement to provide IT infrastructure and application services to Procter & Gamble.

P&G's ITSM program was initiated and matured within the group that was outsourced. With both the work and many employees moving to HP, P&G's entire Service Management program began losing momentum. After assessing the retained IT work, the ITSM program was revitalized to encompass proactive management of suppliers and IT services, focusing on the value of solid system platforms to create an environment for continuous process improvement and innovation. This presentation covers the challenges of sustaining an ITSM program in the midst of a major IT outsourcing effort.

---

[2] data from IDC documentation on ITIL
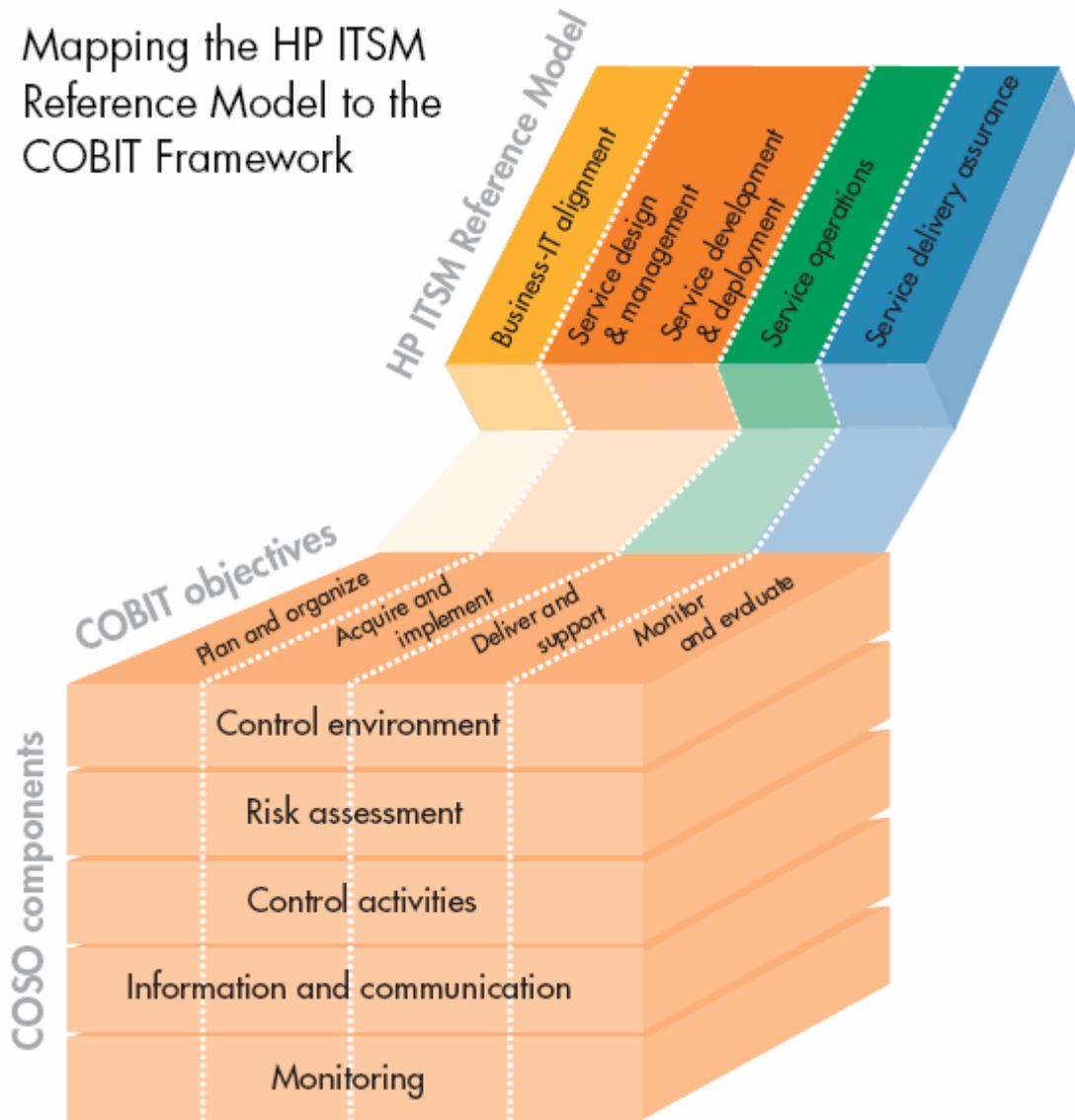
Conclusions and Findings

This paper provides a starting point for organizations thinking the risk of IT outsourcing and wishing to enhance their IT service performance more effective under ITIL ITSM framework.

As mention above, IT security issue always exist and cannot be readily transferred by outsourcing to third party.   Risk could not be forecasted, risk should be managed.   IT Service Management concept of ITIL is more than simply meeting agreed-upon service levels.   It also means ensuring that risks are managed, that users have the information to make best use of services (and change services when necessary), and that services properly support the needs of the business.

From the IT outsourcing scenario, we could see more risk control opportunities for business. In order to pursue the high stabilization of IT services, enterprise should use a useful framework to getting the better control of outsourcing deal to eliminate the risk: data lost, betray confidential information, unstable infrastructure…etc.   Hence, the requirement for high quality services and the push to get IT organizations to think and communicate in terms business understands is the reason behind the growth of the ITIL.

Appendix 1 – Mapping the HP ITSM reference model to the COBIT framework

Mapping the HP ITSM Reference Model to the COBIT Framework

Appendix 2 - 16 key IT processes of HP ITSM reference model

Business - IT Alignment

- Manage business relationships
- Interface with customers
- Understand business and customer requirements
- Formulate an IT strategy that optimizes IT added-value

Operations Bridge

- Manage customer satisfaction
- Run services
- Monitor and maintain the service infrastructure
- Resolve incidents and disseminate information
- Proactive problem prevention
- Generate service and infrastructure reports

Service Delivery Assurance

- Document and track service infrastructure information
- Document infrastructure attributes and relationships
- Evaluate and control changes

Service Design & Management

- Translate IT strategy into planned IT services
- Create detailed service design specifications
- Define and manage service levels within financial constraints via service level agreements
- Provide security for infrastructure and data

Service Development & Deployment

- Develop and test services
- Deploy services according to service design

Reference:

1.   Raffoul, Wissam. (2002) "The road to outsourcing success."ZDNet Tech Update, provided by

      Meta Group, March 4, 2002. Article available online as of May 28, 2003 at

      http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2851971,00.html

2.   Corbett and Associates (2002). "Outsourcing's Next Wave". Article available online as of

      May 28, 2003, at: http://www.firmbuilder.com/articles/19/50/752/

3.   Lui, J. (2003). "Advice to outsourcers: It's good to talk", Special to CNET News.com, posted

      on March 31, 2003. Available as of 28 June 2003 at:

      http://news.com.com/2100-1011-994771.html

4.   Reining in Outsourcing Risk

       http://www.strategy-business.com/sbkwarticle/sbkw051130?pg=all

5.   HP ITSM and HP OpenView: an approach to attaining Sarbanes-Oxley compliance
http://www.managementsoftware.hp.com/regions/americas/initiatives/sarbanes_oxley_wp.pdf