COBIT - ITIL mapping for Business Process Continuity Management

Melita Kozina
Faculty of Organization and Informatics
University of Zagreb
Pavlinska 2,42000 Varaždin, Croatia
melita.kozina@foi.hr

Abstract. *Business Continuity Management (BCM) covers risk analysis and management so that the organization can ensure a provision of service at all times. BCM aims to reduce risks and develops plans for restoring business activities if they are interrupted by a disaster.CobIT and ITIL are two specific IT best practices and standards that are becoming widely adopted around the world to better manage the quality and reliability of IT in business. CobiT can be used at the highest level of IT governance, providing an overall control framework based on an IT process model. There is also a need for detailed, standardised practitioner processes. Specific practices and standards, such as ITIL, cover specific areas and can be mapped to the CobiT framework.The purpose of the paper is to analyze and describe these standards, especially their mapping for improved performance, value transparency and increased control over BCM activities. So, ITIL processes may be used to achieve and demonstrate compliance with CobiT control objectives for BCM process.*

Keywords. Business Continuity Management (BCM), IT Service Continuity Management (ITSCM), CobIT, ITIL, Mapping Best Practices.

1 Introduction

Business Continuity Management (BCM) covers risk analysis and management so that the organization can ensure a provision of service at all times. BCM aims to reduce risks and develops plans for restoring business activities if they are interrupted by a disaster. IT Service Continuity Management (ITSCM) is part of the overall BCM process and depends on the information provided by the BCM process. Successful implementation of ITSCM requires the understanding and support of the whole organization, especially the essential support of senior business managers and directors.

Every enterprise needs to tailor the use of standards and practices to suit its individual requirements. Users need more guidance on how to integrate the leading global frameworks and other practices and standards. In response to this question, this paper analyses and describes the mapping of CobiT and ITIL for successful implementation, improved performance and increased control over BCM/ITSCM process and their activities. So, ITIL processes may be used to achieve and demonstrate compliance with CobiT control objectives for BCM process.

CobiT does not include process steps and tasks because, although it is oriented towards IT processes, it is a control and management framework rather than a process framework. CobiT focuses on what an enterprise needs to do, not how it needs to do it. ITIL is based on defining best practice processes for IT service management and support, rather than on defining a control framework. It focuses on how an enterprise needs to do for service management aspects [7].

2 ITSCM process model

The objective of ITSCM is to support the overall Business Continuity Management (BCM) by ensuring that necessary IT infrastructure and IT service can be restored after a disaster (incident) within optimal time limits and costs. A disaster is much more serious than an incident. It is a business interruption and it can include fire, burglary, water damage, vandalism and violence, hardware failure, Internet, terrorist attacks, etc. Today, the businesses are increasingly dependent on IT services and it is very important to analyze how to realize business continuity.

Businesses with an ITSCM process have the following benefits[4]:

a) they can manage the recovery of their systems;
b) they lose less service avalilability time and offer better continuity to the users;
c) they minimize the interruption to their business activities.

ITSCM process model (based on BCM) model and its main stages (activities) is shown on Fig.1.

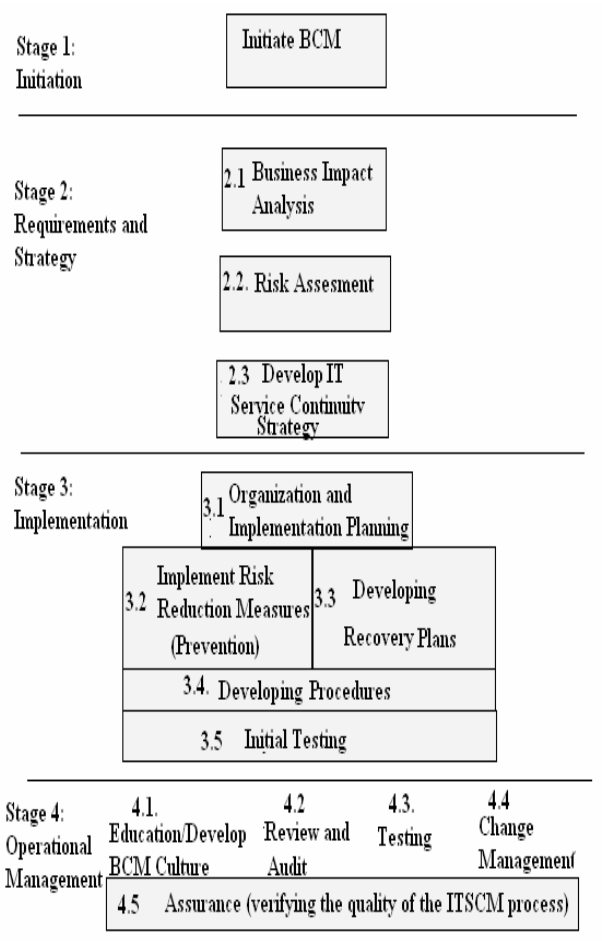

Figure 1. ITSCM process model (based on ITIL BCM model)

ITSCM/BCM activities will be decribed in chapter related to CobIT and ITIL mapping the BCM process. ITSCM process has several important objectives through presented stages.

- assessing the risk and impact of the interruption of IT services following disaster;
- identifying services critical to the business that require additional prevention measures;
- developing, testing and maintaining a recovery plans;
- defining the approach to be used to restore the IT services;
- defining periods within which services have to restored;
- taking measures to prevent, detect, prepare for the effects of disasters or to reduce their impact.

3 CobIT

CobiT (Control Objectives for Information and related Technology), published by ITGI, is a globally accepted framework for IT governance. IT governance addresses these main areas of IT activity as follows[2]:

- Strategic alignment, with a focus on aligning IT with the business solutions;
- Value delivery, concentrating on optimising costs and proving the value of IT;
- Risk management, addressing the safeguarding of IT assets (including project investments), disaster recovery and continuity of operations;
- Resource management, optimising knowledge and IT infrastructure;
- Performance measurement, tracking project delivery and monitoring IT services.

CobiT enables business executives to better understand how to direct and manage the enterprise's use of IT and the standard of good practice to be expected from IT providers. CobiT provides the tools to direct and control IT-related activities [1].

The CobIT framework includes the folowing components:

- **Framework** - explains how CobiT organises IT governance management and control objectives and good practices by IT domains and processes, and links them to business requirements; IT processes are grouped into four domains: *Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate*.
- **Process descriptions** for each of 34 IT processes;
- **Control objectives**—provide generic best practice management objectives for IT processes;
- **Management guidelines**—offer tools to help assign responsibility and measure performance
- **Maturity models**—assess the maturity level for each of 34 IT processes as well as the whole IT organization. This assessment is the basis of benchmarking in relation to other IT

organizations, aimed at improving the IT organization in question.

The enterprise requires IT management framework as its main support in order to achieve the IT business value. Fig. 2 shows the management of IT organization using the CobIT method. Fig.3 shows the CobIT framework [3].

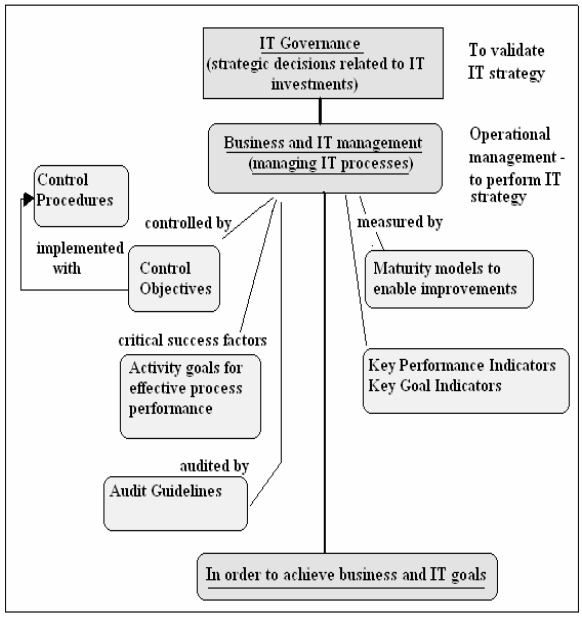

Figure 2. COBIT for planning and management of IT organization

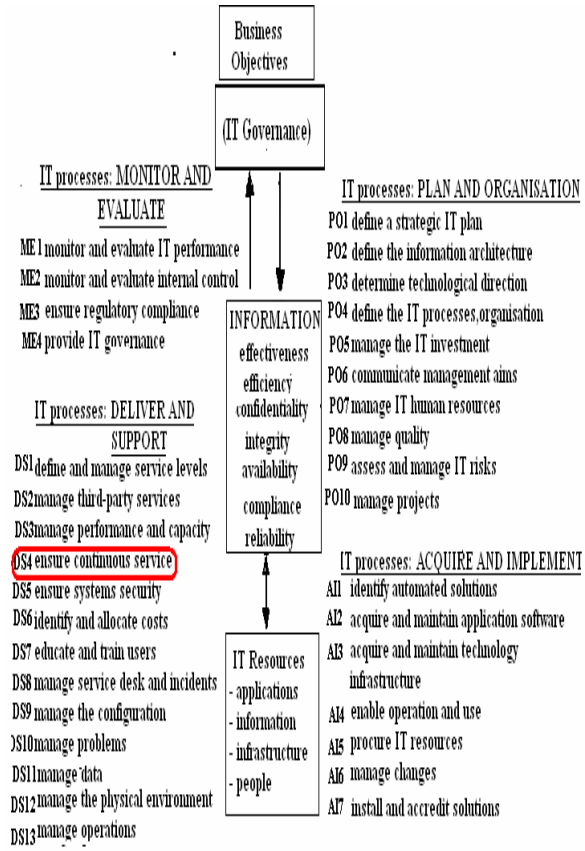

Figure 3. COBIT framework

4 ITIL

Except CobiT there is another useful and supportive mechanism for planning and management of IT processes, as well as the BCM process.

ITIL (Information Technology Infrastructure Library) standard, published by the UK government, ensures a consistent best practice concept for setting up the IT service management processes built into the IT organization. Some of ITIL benefits for customer/user are:

- The IT services are described better in more detail;
- The quality, availability, reliability and cost of the services are managed better;
- The provision of IT services becomes more customer-focused.

Some of ITIL benefits for IT organization are:

- The IT organization develops a clearer structure, more focused to the corporate objectives;
- The IT organization has better control of the IT infrastructure and services;
- The ITIL best practices support the introduction of quality management system (example ISO 9000; Six Sigma; etc);
- ITIL provides the quality internal communication and communication with suppliers.

Potential problems with using ITIL are:

- The implementation can take a log time and require significant effort and costs;
- A successful implementation requires the involvement of personnel at all levels in the organization;
- Improvement in the provision of services and cost reductions are insufficiently visible;
- Insufficient investment in adequate education and support tools.

IT service management is concerned with planning, sourcing, designing, implementing, operating, supporting and improving IT services that are appropriate to business needs. IT Service Management provides the strategic alignment between the business company and IT organization (function), shown on Fig.4 [5].

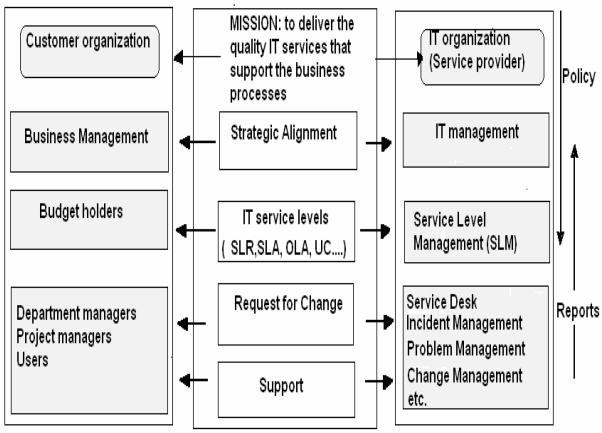

Figure 4. IT Customer Relationship Management

In new context of ITIL (ITIL V3), the key processes have been updated, but more significantly. ITIL now describes IT service management functions, activities and organisational structure; strategic and sourcing concerns; and integration with the business. In ITIL V3, the most significant development has been the move from a process-based framework to a more comprehensive structure reflecting the life cycle of IT services. The processes and functions within the life cycle of IT services are shown on Fig.5 [6].

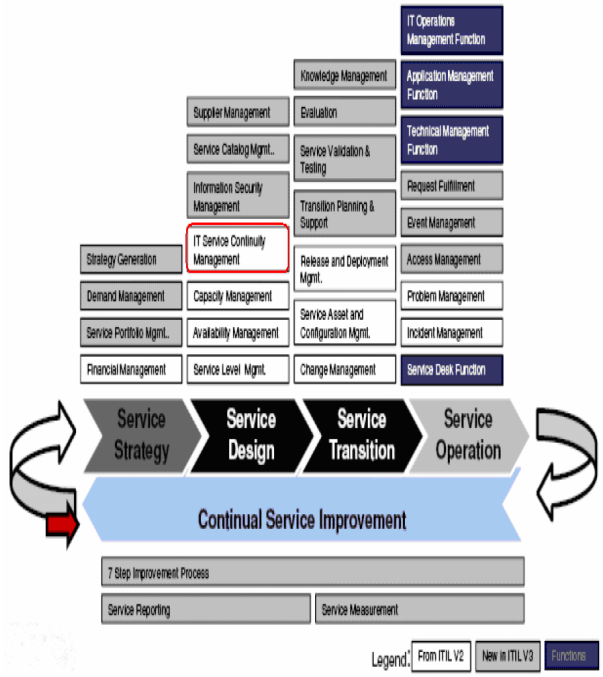

Figure 5. ITIL V3 processes and functions

5 CobIT - ITIL mapping for BCM

IT best practices need to be aligned to business requirements and integrated with one another and with internal procedures. According to Gartner many of the CobiT processes , especially those in the Delivery and Support (DS) domain, map well onto one or more ITIL processes [8]. CobiT can be used at the highest level, providing an overall control framework based on an IT process model that should suit every organisation generically. Specific practices and standards such as ITIL cover particular areas and can be mapped to the CobiT framework. In the paper, this mapping is analyzed within the BCM/ITSCM process.

As mentioned, ITSCM process (based on BCM) is very important process for the company and its planning and management require significant efforts and resources. The purpose of the paper is to analyze and describe CobIT and ITIL mapping for improved performance, value transparency and increased control over BCM activities.ITIL processes may be used to achieve and demonstrate compliance with CobiT control objectives for BCM process.

To better understand mapping amongst ITIL and CobIT over the BCM process, each of the 10 CobiT control objectives for DS4 (Ensure Continuous Service) and relevant key areas within control objectives, has been mapped to specific ITIL activities/processes. Focus was on ITIL ITSCM process and its 4 stages of activities (shown on Fig.1), as well as other relevant ITIL processes (availability management; capacity management, change management, etc.). This mapping is shown on Fig.6.

The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, utilising offsite backup storage and providing periodic continuity plan training. An effective continuous service process minimises the probability and impact of a major IT service interruption on key business functions and processes.

Organisations wishing to adopt IT best practices need an effective management framework that provides an overall consistent approach and is likely to ensure successful business outcomes when using IT to support the enterprise's strategy.

Implementation of best practices is very complex process and requires the detailed planning process. Additional, it should be consistent with the enterprise's risk management and control framework, appropriate for the enterprise, and integrated with other methods and practices that are being used.

CobIT DS4 Control Objectives	KEY AREAS for control objectives (DS4)	ITIL V3 processes and activities (focus on ITIL ITSCM process)
DS4.1 IT continuity framework	**a) Enterprisewide consistent approach to continuity management** - to develop IT continuity framework to support BCM using a consistent approach - to analyze the reguired infrastructure - to drive the development of disaster recovery and IT contigency plans - to define organizational structure for BCM (roles, tasks, service providers, planning processes that create the rules and structures to document, test and execute the recovery and IT contigency plans) - to identify the critical resources and their monitoring and the principles of backup.	**ITSCM-Stage 1: Initiation-initiate ITSCM** -to define the ITSCM policy (awareness due to ITSCM) -to define ITSCM scope and relevant areas (insurance requirements; quality standards; security management; methods for risk assessment and business impact analysis) - to define management structure with assigned responsibilities and process structure - to allocate resources - setting up the project organization
DS4.2 IT continuity plans	**a) Continuity plans based on risk assessment and business impact analysis** **b) Continuity plans have to address requirements for resilience, alternative processing and recovery capability of all critical IT services.**	**ITSCM-Stage 2: Requirements and Strategy** **2.1. Business Impact Analysis** - to define the reasons for including ITSCM in BCM (protecting business processes, rapid service recovery, maintaining market share and profitabiliy, customer satisfaction, etc.) - to identify the potential impact of a serious disruption of IT services; business can survive for some time and the focus will be on ***restoring services***; in other cases, business cannot operate without IT services and the focus will be on ***prevention***; most business have a balance between these two cases. - to analyze the IT services that are essential for the business and that must be available according to **SLA** - to assess the dependencies between services and IT resources; ***availability management*** information is used to analyze the extent to which IT resources support IT service; ***capacity management*** provides information about the required capacity; these information is useful for recovery options for each IT service. **2.2. Risk Assessment** - to identify the relevant IT components (assets) (the purpose of each component must be documented). - to analyze the threats to those assets and the likelihood (high, medium,low) that a disaster will occur. - to identify the vulnerabilities of the assets; classified – high, medium, low. - to evaluate the threats and vulnerabilities in the context of the IT components in order to estimate the level of risks. **2.3. Developing IT Service Continuity Strategy** - most business will focus to a balance between ***risk reduction (prevention) and recovery planning.*** - prevention measures can be taken on the basis of the risk analysis; the measures focuse to
		reduce the likelihood or impact of contingencies. - other risks are covered by recovery planning/options (paper-based backup routines; reciprocal arrangements; cold, warm or hot stand by recovery); **ITSCM-Stage 3: Implementation** **3.1. Once the ITSCM strategy has been defined, the ITSCM has to be implemented and the plans for the IT facilities have to developed in detail.** - an organization has to set up to implement the ITSCM process. - this could include management, coordination and recovery teams for each service. - in the case of the business recovery process, for example, the following plans have to be activated: (accommodation and service plan; computer system and network plan; telecommunications plan; security plan; personnel plan; financial plans.) **3.2.Defining prevention measures** to reduce the impact of an incident are taken together with availability management and together with **stand-by agreements** include the following activities: a) negotiating off-site recovery facilities with third parties b) maintaining and equipping the the recovery facility c) purchasing and installing stand-by hardware (dormant contracts), etc. **3.3.Developing recovery plans** - a typical recovery-planning problem relates to changes in the infrastructure and the SLA - **the recovery plan should include all elements relevant to restoring the business activities and IT services; it includes:** a) **introduction** that describes the structure of the plan and recovery facilities b) **updating** that defines the maintaining the plan, tracks changes to the infrastructure c) **recovery initiation** that describes when the plan is invoked d) **contingency classification** (seriousness –minor, medium, major; duration – day, weeks; damage (minor, limited, serious) e) **special section:** *administration* (how and when is the plan invoked; wchich managers and personnel are involved; where is the control center); *IT infrastructure* (hardware, software, telecommunications to be provided by the recovery system; recovery procedures;dormant contracts); *personnel* required at the recovery facility; *security* (plans for protection against burglary, fires, explosions, etc.); *recovery sites* (information about contracts, security, transport, personnel with specific function, etc.); *restoration* (procedures to restore the normal situations; different conditions related to procedures)
		3.4.Developing procedures can inlude installing and testing hardware and software components; restoring applications, databases and data, etc.
DS4.3 Critical IT resources	**a) Focus on critical infrastructure in the IT continuity plan to build in resilience and establish priorities in recovery** situations; **b) Consider resilience, response, recovery requirements**	**ITSCM-Stage 2: Requirements and Strategy** **2.3. Developing IT Service Continuity Strategy (cooperation with Availability Management)** - to consider prevention measures and especially recovery options for IT services (return to a manual-paper based system for minor services; *reciprocal arrangements*; *gradual recovery* (cold stand-by; example 72 hours); *intermediate recovery* (warm stand-by; 24-72 hours); *immediate recovery* (hot stand-by; immediate or less than 24 hours); combinations of options.

CobIT DS4 control objectives	KEY AREAS for control objectives (DS4)	ITIL V3 processes and activites (focus on ITIL ITSCM process)
DS4.4 Maintenance of the IT continuity plan	Changing control to reflect changing business requirements	**ITSCM-Stage 4: Operational Management (ongoing operation)** **4.2 Review and Audit** - plans should be reviewed regularly every time there is any change to the IT infrastructure or the changes in business and IT strategy; it must be implemented under the direction of Change Management **4.4. Change management** - the impact of any change to the recovery plan is analyzed
DS4.5 Testing of the IT continuity plan	a) Regular testing to ensure that IT systems can be effectively recovered b) Implementing action plan according to the test results	**ITSCM-Stage 3: Implementation** **3.5. Initial testing of the plans, procedures and technical components** involved within ITSCM. **ITSCM-Stage 4: Operational Management (ongoing operation)** **4.3. Testing** - the recovery plan must be tested regulary in order to identify weaknesses in the plan or changes that were overlooked.
DS4.6 IT continuity plan training	- Regular training for all concerned parties	**ITSCM-Stage 1: Initiation** - training must be provided to ensure that personnel are prepared to realize stage 2 of the ITSCM process (Requirements and Strategy) **ITSCM-Stage 3: Implementation** **ITSCM-Stage 4: Operational Management (ongoing operation)** **4.1. Education/Develop BCM culture**
DS4.7 Distribution of the IT continuity plan	- Proper and secure distribution to all authorised parties	**ITSCM-Stage 3: Implementation** (developing plans and procedures; their adequate distribution) **ITSCM-Stage 4: Operational Management (ongoing operation)** - plans must be accessible under all disaster scenarios
DS4.8 IT services recovery and resumption	- Planning the actions for period when IT is recovering and resuming services - Business understanding and investment support	**ITSCM-Stage 4: Operational Management (ongoing operation)** **- cooperation with ITIL Availability Management**
DS4.9 Offsite backup storage	- Offsite storage of all critical media, documentation and resources needed in collaboration with business process owners	**ITSCM-Stage 2: Requirements and Strategy** - information backup
DS4.10 Post-resumption review	-Regular management assessment of plans	**ITSCM-Stage 4: Operational Management (ongoing operation)** **4.5. Assurance** – it means verifying that the quality of the process (procedures and documents) are adequate to meet the business requirements.

Figure 6. CobIT – ITIL mapping for IT Service Continuity Management process (based on BCM) (Aligning CobIT 4.1. control objectives and ITIL V3 processes (activites) for ITSCM/BCM, source: Author)

6 Conclusion

As business are increasingly dependent on IT services, the objective of IT Service Continuity Management (ITSCM) is to support the overall Business Continuity Management (BCM) by ensuring that required IT infrastrucure (IT services) can be restored within optimal costs and time after a disaster. The risk analysis is very important within this process because once the risk to the business (not just the risk to the IT services), has been identified, investments can be made measures for prevention and recovery plans.

The planning and management of ITSCM/BCM process requires many efforts and support of the whole organization, especially directors and senior business managers. The implementation of this process can include different problems related to *resources, commitment, access to recovery facilities*, *difficult estimating the damage, budgeting, no business manager commitment, delay, IT department that must be guided by the business requirements, lack of BCM awareness.*

The paper focuses on two specific practices and standards that are becoming widely adopted around the world:

a) ITIL V3—published by the UK government to provide a best practice framework for IT service management and

b) CobiT 4.1—published by ITGI and positioned as a high-level governance and control framework.

CobiT define what should be done and ITIL

providing the how for service management aspects. These practices and standard can be mapped for improved performance, value transparency and increased control over ITSCM/BCM activities and for diminishing above described problems.This was the purpose of the paper.

In general, the use of IT has the potential to enterprise success, provides opportunities to obtain a competitive advantage and offers a means for increasing productivity. Best practices and standards help enable effective governance of IT activities as well as the adequate benchmarking of the whole IT performance and use in the company.

References

[1] Haes,D.S.,Grembergen,V.W.: **IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group**, Proceedings of the 38th Hawaii International Confernce on System Science,2005.

[2] Haes, S.D. & Grembergen, W.V. (2004). **IT Governance ad Its Mechanisms**, *Information Systems Control Journal,* Vol.1, 2004, pp.27-33, ISACA, ISSN: 1526-7407.

[3] ITGI IT Governance Institute, **CobiT 4.1,** USA, 2007.

[4] OGC Office of Government Commerce, **Introduction to ITIL,** U.K., 2005.

[5] OGC Office of Government Commerce, **Planning to Implement Service Management,** U.K., 2002.

[6] OGC Office of Government Commerce, **The Official Introduction to the ITIL V3 Service Lifecycle,** U.K., 2007.

[7] Salle, M.:**IT Service Management and IT Governance: Review, Comparative Analysis and their Impact on Utility Computing,** available at: http://www.hpl.hp.com/techreports/ 2004/HPL-2004-98.pdf, Accessed:10th May2009

[8] **Combine CobiT and ITIL for Powerful IT Governance,** Gartner, Tactical Guidelines, TG-16-1849, Research Note 10 June 2002.

[9] **CobiT Mapping – Overview of International IT Guidance**, IT Governance Institute, available at: http://www.itgi.org, Accessed: 25th May 2009.

[10] **CobiT Mapping: Mapping of ITIL V3 With CobiT 4.1**, available at: http://www.isaca.org, Accessed: 30th May, 2009.