Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations

Preprint · June 2018

CITATIONS
0

READS
3,614

3 authors, including:

Shamsul Sahibuddin
Universiti Teknologi Malaysia
138 PUBLICATIONS **1,156** CITATIONS
SEE PROFILE

Mohammad Sharifi
Universiti Teknologi Malaysia
2 PUBLICATIONS **4** CITATIONS
SEE PROFILE

Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations

Shamsul Sahibudin
shamsul@utm.my
shamsul@fsksm.utm.my

Mohammad Sharifi
sharifi@citycampus.utm.my
sharifi1400@yahoo.com

Masarat Ayat
ayat@citycampus.utm.my
nahadineh_122@yahoo.com

Centre for Advanced Software Engineering (CASE), University Teknologi Malaysia
81310 UTM,skudai,johor,Malaysia

Abstract

Several frameworks, tools and standards have been included in IT management systems, in organizations. However, on their own, they are not comprehensive enough to serve as efficient IT management system. This paper reviews two established frameworks, i.e. ITIL, COBIT and a standard, ISO/IEC 27002 focusing on their similarities and differences. It then proposes a comprehensive framework by integrating the three general framework and standards into an IT framework that could be used in every company.

1. Introduction

Management is an attempt to direct and control a group of one or more people or entities for the purpose of coordinating and harmonizing them towards accomplishing a special goal. At present Management encompasses several dimensions like human resources, financial resources and technological resources. One new area of management is Information technology management (or IT management). It is a combination of two branches of study, information technology and management [1].

'Information technology' has several definitions from different perspectives:

From the first perspective, IT systems are applications and infrastructures which are components of a larger product. They enable or are embedded in processes and services.

From the second perspective, IT is an organization with its own set of capabilities and resources. IT organizations can be of various types such as business functions, shared services units and enterprise-level core units.

From the third perspective, IT is a category of services utilized by business. They are typically IT applications and infrastructure that are packaged and offered as services by internal IT organizations or external service providers. In this perspective IT costs are treated as business expenses.

From the fourth perspective, IT is a category of business assets that provide a stream of benefits for their owners, including but not limited to revenue, income and profit. In this perspective IT costs are treated as investments [2].

All definitions emphasize the importance of IT in the organizations. Therefore it is crucial to manage and implement IT in the organizations. There are several standards, tools, frameworks and best practices to manage and maintain IT services. The most applicable and widely used such standards are ISO/IEC 27002 in information security [3], COBIT [4], *ISO 20000[5]* and ITIL [6]. Every standard, tool and framework has its strength and its limitation. Hence, it is better to combine them to make a comprehensive IT framework in the organizations. Based on previous studies the best combination should be between laying ITIL, COBIT and ISO/IEC17799 together [7]. But ITIL de-facto standard and ISO/IEC 17799 standard recently has been refreshed and changed.

This paper, will firstly provide a ITIL, COBIT and ISO/IEC 27002 will be stated. Then based on these three frameworks and standards a comprehensive framework will be proposed.

2. ITIL

ITIL (Information Technology Infrastructure Library) is a de-facto standard which introduced and distributed by Office of Government Commerce (OGC) in UK and includes all IT parts of organizations [8]. At present ITIL is the

most widely accepted approach to IT Service Management in the world. It has an iterative, multidimensional and lifecycle form structure. ITIL has an integrated approach as required by the ISO/IEC 20000 standard with following guidance: [9]

■ Service Strategy

The Service Strategy provides guidance on how to design, develop and implement service management from organizational capability perspective and strategic asset. It provides guidance on the principles underpinning the practice of service management which are useful for developing service management policies, guidelines and processes across the ITIL service lifecycle. Service Strategy guidance is applicable in the context of other parts of ITL lifecycle. Service Strategy covers these parts of IT systems: the development of markets, internal and external, service assets, service catalogue and implementation of strategy through the service lifecycle.

Service Strategy includes these processes:

- Financial Management
- Service Portfolio Management
- Demand Management [10].

■ Service Design

It is guidance for the design and development of services and service management processes. It covers design principles and methods for converting strategic objectives into portfolios of services and service assets. The scope of Service Design is includes the changes and improvements necessary to increase or maintain value to customers over the lifecycle of services, the continuity of services, achievement of service levels and conformance to standards and regulations. It guides organizations on how to develop design capabilities for service management. Service Design includes these processes:

- Service Catalogue Management
- Service Level Management
- Capacity Management
- Availability Management
- IT service Continuity Management
- Information Security Management Supplier Management, Application Management
- Data and Information Management Business Service Management [11].

■ Service Transition

It is guidance for the development and improvement of capabilities for transitioning new and changed services into operations. Service Transition provides guidance on how the requirements of Service Strategy encoded in Service Design are effectively realized in Service Operation while controlling the risks of failure and disruption. This part of ITIL framework combines practices in release management, program management and risk management and places them in the practical context of service management.

Service Transition processes are:

- Change Management
- Service asset and Configuration Management
- Release and deployment Management
- Knowledge Management
- Stakeholder Management
- Transition Planning
- Support and Service Evaluation [12].

■ Service Operation

Service Operation tries to embody practices in the management of Service Operation. It includes guidance on achieving effectiveness and efficiency in the delivery and support of services so as to ensure value for the customer and the service provider. Strategic objectives are ultimately realized through Service Operation, therefore making it a critical capability.

It processes are:

- Event Management
- Incident Management
- Request Management
- Problem Management
- Access management [13].

■ Continual Service Improvement.

This is including of instrumental guidance in creating and maintaining value for customers through better design, introduction and operation of services. It combines principles, practices and methods from quality management, Change Management and capability improvement. Organizations learn to realize incremental and large-scale improvements in service quality, operational efficiency and business continuity.

Its processes are:

- The 7-Step Improving Process
- Service Level Management [14].

3. COBIT

The Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for information technology management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992. COBIT was released and used primarily by the IT community. Later Management Guidelines were added, and COBIT became the internationally accepted framework for IT governance and control[15].

COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.

In its latest edition, COBIT has 34 high level objectives that cover 215 control objectives categorized in four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.

The COBIT mission is to research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors. Managers, auditors, and users benefit from the development of COBIT because it helps them understand their IT systems and decide the level of security and control that is necessary to protect their companies' assets through the development of an IT governance model. COBIT covers four domains:

▪ Plan and Organize

The Planning and Organization domain covers the use of technology and how best it can be used in a company to help achieve the company's goals and objectives. It also highlights the organizational and infrastructural form IT is to take in order to achieve the optimal results and to generate the most benefits from the use of IT. Here is lists of the high level control objectives for the Planning and Organization domain.

- Define a Strategic IT Plan
- Define the Information Architecture
- Determine Technological Direction
- Define the IT Processes, Organization and Relationships
- Manage the IT Investment
- Communicate Management Aims and Direction
- Manage IT Human Resources
- Manage Quality
- Assess and Manage IT Risks
- Manage Projects

▪ Acquire and Implement

The aim is to identify its IT requirements acquiring the technology and to implement it within the company's current business processes. This domain also addresses the development of a maintenance plan that a company should adopt in order to prolong the life of an IT system and its components. Here is list of the high level control objectives for the Acquisition and Implementation domain.

- Identify Automated Solutions
- Acquire and Maintain Application Software
- Acquire and Maintain Technology Infrastructure
- Enable Operation and Use
- Procure IT Resources
- Manage Changes
- Install and Accredit Solutions and Changes

▪ Delivery and Support

This domain tries to manage delivery services which include:

- Define and Manage Service Levels
- Manage Third-party Services
- Manage Performance and Capacity
- Ensure Continuous Service
- Ensure Systems Security
- Identify and Allocate Costs
- Educate and Train Users
- Manage Service Desk and Incidents
- Manage the Configuration
- Manage Problems
- Manage Data
- Manage the Physical Environment
- Manage Operations

▪ Monitor and Evaluate

The Monitoring and Evaluation domain deals with a company's strategy in assessing the needs of the company and whether or not the current IT system still meets the objectives for which it was designed and the controls necessary to comply with regulatory requirements. Monitoring also

covers the issue of an independent assessment of the effectiveness of IT system in its ability to meet business objectives and the company's control processes by internal and external auditors. The following table lists the high level control objectives for the Monitoring domain

- Monitor and Evaluate IT Processes
- Monitor and Evaluate Internal Control
- Ensure Regulatory Compliance
- Provide IT Governance[16].

4. ISO/IEC 27002

This is an information security management system (ISMS) standard which is the Code of Practice for Information Security Management. It lists security control objectives and recommends a range of specific security controls. Organizations that implement an ISMS in accordance with the best practice advice in ISO/IEC 27002 are likely simultaneously to meet the requirements of ISO/IEC 27002, but certification is entirely optional (unless mandated by the organization's stakeholders)[17].

5. ITIL related to COBIT

The strength within ITIL is the way processes are described with different activities and flowcharts to use for target implementation. Cost/Benefit and implementation issues are also described. There are also guidelines for reviews and Critical Success Factors, but these issues are better described in COBIT. First of all COBIT is defined by the IT-audit community as a framework highly suitable for authority. COBIT is also stronger when it comes to management issues where "Management Guidelines" provides the implementer with a reference where Critical Success Factors are described together with Key Goal Indicators, Key Performance Indicators and Capability Maturity Models (CMM).

When ITIL is benchmarked with COBIT, it has been found that they correspond with each other to a high degree, especially, when the processes of COBIT are ITIL based as in its latest version. In spite of different words used for the same issue but they cover the same problem. It is only for Incident Management in ITIL that there is not any equivalent in COBIT. This however, does not mean that it is not covered at all; instead it may be covered in other parts of the framework or with a different approach [18]. As shown in Table 1.

Therefore it is better to borrow Concepts/process, Activities, Cost/Benefits and Planning to Implementation from ITIL standard and Audits from COBIT to design a comprehensive framework.

Table 1: Compare ITIL and COBIT

ITIL	COBIT
Incident Management	Manage Problems and Incidents
Problem Management	Manage Problems and Incidents
Configuration Management	Manage and Configuration
Change Management	Manage Change
Release Management	Manage Changes and Configuration
Service Level Management	Define and Manage Service Levels
Financial Management for IT Services	Identify and Allocate Costs
Capacity Management	Manage Performance and Capacity
Service Continuity Management	Ensure Continuous Service
Availability Management	Manage Performance and Capacity

6. ITIL related to ISO ISO/IEC 27002

As already mentioned, ISO/IEC 27002 is used for information security and not just IT issues. With such broad objectives it is apparent that ISO/IEC 27002 does not correspond with ITIL as much as ITIL does with COBIT. ISO/IEC 27002 main straight is in its application for ensuring overall security at all levels within an organization.

Problem Management and Configuration Management in ITIL have not any equivalent in ISO 27002. Configuration Management has a huge impact on the IT environment and it should be handled in a secure manner. In addition in ISO/IEC 27002 security is characterized as the preservation of Confidentiality, Integrity and Availability. In ITIL Availability is about quality aspects such as reliability, maintainability, serviceability & resilience. Another important finding in the benchmark is that financial issues are not handled at all in ISO/IEC 27002; instead it is about only risk management, i.e. the implementer should mitigate risks to avoid costs.

ITIL, on the other hand, is about financing and cost allocation for the delivery of IT-services.

Therefore it is better to borrow Information Security process from ISO/IEC 27002 in designing a comprehensive framework.

Conclusion

In every organization today, IT services must be delivered in a cost efficient manner, mitigating security risks and complying with legal requirements. The equation is difficult to handle and in some cases it seems like an impossible mission. To be able to survive in this environment a combination of ITIL, COBIT and ISO/IEC 27002 can be valuable for organization targets. Implementers should use ITIL to define strategies, plans and processes, use COBIT for metrics, benchmarks and audits and use ISO/IEC 27002 to address security issues to mitigate the risks as below in Table 2.

Table 2: Adapting ITIL with COBIT and ISO/IEC27002

ITIL	COBIT	ISO/IEC 27002
Concepts/process	Critical Success Factors	Information Security
Activities	Metrics(CSF,KPI)	
Cost/Benefits	Benchmarking(CMM)	
Planning for Implementation		
	Audit	

Acknowledgment:

The authors would like to thank all anonymous researchers involved in gathering information to organize ITIL ,COBIT and ISO/IEC 27002 standards.

References

[1] wikipedia, Management, Business and Economics WikiProject., *3 July 2007, http://en.wikipedia.org/wiki/Management.*

[2] Sharon Taylor, S.Lacy, I.Macfarlane, ITIL:Service Transition,TSO publications.Norwith,UK,2007

[3]wikipedia, ISO-IEC-27002:,ISO standards, November 2007 , http://www.bsi-global.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes.

[4] Wikipedia, COBIT:2005,Quality Management, 24 November 2007, http://en.wikipedia.org/wiki/COBIT..

[5] Wikipedia, ISO/IEC 20000:2005, ISO/IEC standards,October 2007, http://en.wikipedia.org/wiki/ISO_20000.

[6] Wikipedia,ITIL v3, Information technology management , 24 November 20, http://en.wikipedia.org/wiki/ITIL_v3.

[7] John Wallhoff, Combining ITIL with COBIT and 17799, 15 October 2007,www.scillani.com\COBIT\Scillani%20Article%20Combining%20ITIL%20with%20Cobit%20and%2017799.

[8]ITIL forum(2007), Information Technology Infrastructure Library ver 3, From Wikipedia, the free encyclopedia

[9]Jan van Bon,M.Pieper,A.Veen,T.Verheijen,Best Practices: Introduction to ITIL,TSO Publications,Norwich,June 2007.

[10] Sharon Taylor, M.Iqbal, M.Nieves, ITIL:Service Strategy,TSO publications.Norwith,UK,2007

[11]Sharon Taylor, V. Lioyd,C.Rudd, ITIL:Service Design,TSO publications.Norwith,UK,2007

[12]Sharon Taylor,S. Lacy,I.Macfarlane, ITIL:Service Transition,TSO publications.Norwith,UK,2007

[13]Sharon Taylor, D. Cannon,D.Wheeldon, ITIL:Service Strategy,TSO publications.Norwith,UK,2007

[14] Sharon Taylor, G.Case,G.Spalding, ITIL:Continual Service Improvement,TSO publications.Norwith,UK,2007

[15] Eric Lachapelle, White Paper : "Control Objectives for Information and related Technology ",Veridion Inc.,Montreal, Canada,2 October2007, .www.veridion.net\ITIL+COBIT\cobit_en_wp.pdf,2007.

[16] David Kohrell, CobiT and IT Governance - Elements for building in securityfrom the top, down and thebottom, up,23 October 2007, www.tapuniversity.com

[17] Introduction To ISO 27002 (ISO27002), 27 November 2007,http://www.27000.org/iso-27002.htm

[18] Peter Hill, K. Turbitt, Combine ITIL and COBIT to MeetBusiness Challenges , 9 November 2007, www.bmc.com,\COBIT\BMC_BPWP_ITIL_COBIT_06.pdf