

UNIFICATION OF IT PROCESS MODELS INTO A SIMPLE FRAMEWORK
SUPPLEMENTED BY TURKISH WEB BASED APPLICATION

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF INFORMATICS INSTITUTE
OF
THE MIDDLE EAST TECHNICAL UNIVERSITY

BY

BETÜL AYGÜN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF INFORMATION SYSTEMS

SEPTEMBER 2010

Approval of the Graduate School of Informatics

Prof. Dr. Nazife BAYKAL

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Tuğba TEMİZEL

Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Dr. Elif YILAL

Co-Supervisor

Dr. Ali ARİFOĞLU

Supervisor

Examining Committee Members

Prof. Dr. Nazife BAYKAL

(METU, II) _____

Dr. Ali ARİFOĞLU

(METU, IS) _____

Dr. Elif YILAL

(ERFA) _____

Assoc. Prof. Dr. Ali DOĞRU

(METU, CENG) _____

Assist. Prof. Dr. Erhan EREN

(METU, IS) _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: BETÜL AYGÜN

Signature : _____

ABSTRACT

UNIFICATION OF IT PROCESS MODELS INTO A SIMPLE FRAMEWORK SUPPLEMENTED BY TURKISH WEB BASED APPLICATION

Aygün, Betül

M.S., Department of Information Systems

Supervisor: Dr. Ali ARİFOĞLU

Co-Supervisor: Dr. Elif YILAL

September 2010, 210 pages

Information technology usage has become compulsory for all organizations whether government or private organizations to achieve visibility, compete rivals and execute their missions better. To get desired result from usage of information technology, IT of organization has to be managed well. Up till now, various frameworks are developed to manage it well. Best examples for this kind of frameworks are COBIT and ITIL, containing all processes which can be handled in IT management and becoming widespread through the world. COBIT and ITIL are complementary frameworks rather

than competitors. Due to this reason, organizations must implement both of them instead of choosing one of them. In addition to these, ISO/IEC 27001:2005 which focuses on information security management process is a quite famous IT standard in terms of security.

This thesis provides organizations to meet requirements of these frameworks/standards which are process based frameworks and standards complementary to each other, with a unique implementation by taking unification of processes in a more simple and understandable way. Consequently, it provides reduction in the duplicate work and prevents inconsistencies that may occur. In addition, including CMMI level two requirements motivate the organization to implement higher maturity level of CMMI. Moreover, this study provides organizations to implement ISO 27001 management structure which establish a foundation for extension to technical structure of it. Besides these, this study provides an alignment of frameworks model and COBIT and ITIL which helps organization to trace ITIL and COBIT simultaneously. Lastly by providing a web based application, there exists foundation for knowledge bank of IT processes in Turkish and profile pages for each organization to manage, trace and reach their own IT processes in a digital environment.

Keywords: IT governance, IT service management, IT Frameworks/Standards, IT processes.

ÖZ

TÜRKÇE WEB TABANLI UYGULAMA DESTEĞİ İLE BİRLİKTE BT SÜREÇ MODELLERİNİN DAHA BASİT BİR ÇERÇEVE HALİNDE BİRLEŞTİRİLMESİ

Aygün, Betül

Yüksek Lisans, Bilişim Sistemleri Bölümü

Tez Yöneticisi: Dr. Ali ARİFOĞLU

Ortak Tez Yöneticisi: Dr. Elif YILAL

Eylül 2010, 210 sayfa

Özel ve kamu kurumları olmak üzere bütün organizasyonlarda kendilerini tanıtabilme, rakipleriyle yarışabilme, üstlendiği görevi daha iyi şekilde yürütebilme gibi açılardan bilişim teknolojisinin kullanılmasını zorunlu hale gelmektedir. Bir organizasyon bilişim teknolojisinin kullanımının istenildiği şekilde sonuç vermesi için iyi yönetilmesi gerekmektedir. Şu ana kadar, BT'yi iyi yönetebilmek için çeşitli çerçeveler oluşturulmuştur. Bu çerçeveler için en iyi örnekler BT yönetimini içerisinde ele alınabilecek bütün süreçleri içeren ve dünyada kullanımı yaygınlaşmakta olan COBIT ve ITIL çerçeveleridir. COBIT ve ITIL birbirlerine rakip olmak yerine daha çok birbirlerini tamamlayan çerçeveler olmuşlardır. Bu nedenle, organizasyonlar bu süreçlerden birini

seçmek yerine her ikisini birden kurumlarına uygulama mecburiyeti içindedirler. Bütün bunların yanında, bilgi güvenliği yönetimi sürecine odaklanan ISO/IEC 27001: 2005 Bilgi güvenliği Standardı da güvenlik açısından oldukça ün kazanmış ve başarılı bir standarttır.

Bu tez, birbirlerini tamamlayan süreç temelli bu çerçeve ve standartların daha basit ve anlaşılır bir şekilde süreçlerinin birleştirilerek organizasyonların tek bir uygulama ile bu üç temel çerçeve/standartın gereksinimlerini karşılamasını sağlar. Bundan dolayı, organizasyonlarda farklı kişilerin aynı işlemi ikinci kez yapmasını engellenerek, yapılan işlerde azalma sağlanır ve oluşabilecek tutarsızlıklar engellenir. Buna ek olarak, CMMI olgunluk seviyesi ikinin gereksinimlerini karşılayarak kurumların daha üst olgunluk seviyelerini uygulamak için motive eder. Ayrıca, bu çalışma kurumların ISO 27001 yönetim yapısının da uygulanmasına olanak sağladığı için ISO 27001 teknik kısımlarını karşılayabilmek için bir temel oluşturur. Bütün bunların yanında, tez kapsamında oluşturulan süreçler ile ITIL ve COBIT çerçevelerinin gereksinimleri arasında eşleştirme sağlanarak, süreçler uygulanırken COBIT ve ITIL de eş zamanlı olarak takip edilebilir. Son olarak, web tabanlı bir uygulama ile, BT süreçlerini içeren temel bir Türkçe bilgi bankası ve her organizasyon için kendi süreçlerini dijital ortamda yönetebilme, izleme ve kolayca ulaşma imkanı oluşturulmuştur.

Anahtar Kelimeler: BT yönetim, BT servis yönetimi, BT Çerçeve/Standartlar, BT süreçleri.

To my husband Gürcan

and

To my nephew Ibrahim

ACKNOWLEDGEMENTS

I express sincere appreciation to my supervisor Dr. Ali ARİFOĞLU and to my co-supervisor Dr. Elif YİLAL for their intelligence guidance, insight and constant support throughout my research. They are the people who introduce this research topic and provide their valuable information results from their wide experience during the period of my research.

I am forever grateful to my mother, Fatma, father, Şerif Ali, sister, Yeliz and brother, Ahmet, for their support and patience during this period. I would like to express my sincere thanks to my friends Duygu Fındık, Erkan Er, Gülgün Afacan, Mualla Yılmaz, Münevver Çelik, Seda Erişti, Sinem Derkuş who let me feel their support and faith throughout my thesis study. I am also grateful to all my research assistant friends in Informatics Institute who have any positive touch on my study directly or indirectly. I would like to thank TUBITAK for their scholarship which helped me pursue my master study.

Finally, I offer sincere thanks to my husband Gürcan for his great faith in me and his patience to endure me during this period.

TABLE OF CONTENTS

ABSTRACT	IV
ÖZ.....	VI
DEDICATION	VIII
ACKNOWLEDGEMENTS	IX
TABLE OF CONTENTS	X
LIST OF TABLES	XII
LIST OF FIGURES.....	XIII
LIST OF ABBREVIATIONS	XV
CHAPTER	
1 INTRODUCTION.....	1
1.1 Background	1
1.2 Problem Statement	2
1.3 Objective of Thesis	5
1.4 Outline of Thesis	6
2 FOUNDATIONS OF IT GOVERNANCE AND RELATED RESEARCH.....	7
2.1 What is IT Governance and IT Service Management.....	7
2.2 Framework Types Used	10
2.2.1 COBIT	11
2.2.2 ITIL	14
2.2.3 CMMI.....	18
2.2.4 ISO 27001.....	19
2.3 Unification of IT Management Processes in Literature	21
3 PROBLEM DEFINITION AND OUR PROPOSED SOLUTION.....	22
3.1 Method for Construction Processes	22
3.2 Purpose and Scope of Proposed Solution.....	26

3.2.1	Terms and Definitions	27
3.2.2	Processes	27
3.2.3	Functions	126
4	WEB BASED APPLICATION: IT PROCESSES GUIDE.....	137
4.1	General Description	137
4.1.1	Constraints, Assumptions and Dependencies.....	138
4.2	Design of IT Processes Guide	138
4.2.1	ITPG Database Design	138
4.2.2	ITPG Software Design	139
4.3	An Imaginary Case Study for of IT Processes Guide	148
5	JUSTIFICATION OF PROPOSED SOLUTION	154
5.1	Implemented Processes and Results	155
6	CONCLUSION AND FUTURE WORK	158
6.1	Conclusion	158
6.2	Future Work	159
	REFERENCES	161
	APPENDICES	
A	– The Service Design Package Content	167
B	– Database ER Diagram	168
C	– Process Documentation Template	169
D	– Sample SLA and OLA	171
E	– Service Catalogue Example.....	174
F	– Statement of Requirements (SoR) and/or Invitation to Tender (ITT)	175
G	– Capacity Plan Sample.....	177
I	– Definitions	178
J	– Mapping Framework with COBIT 4.1	184
K	– Mapping Framework with ITILV3	188
L	– Mapping COBIT 4.1 with Framework	193
M	– Mapping ITIL v3 with Framework.....	202
N	– Qualitative Research Questions	209
O	– Figure Explanations.....	210

LIST OF TABLES

Table 3-1 Comparison of COBIT, ITIL and ISO 27001	25
Table 3-2 Coverage types between COBIT and ITIL	25
Table 3-3 General Information about IT management process	30
Table 3-4 General Information about Service Portfolio management process	35
Table 3-5 General Information about Financial management process.....	38
Table 3-6 General Information about Corporate Architecture process	41
Table 3-7 General Information about Risk management process	44
Table 3-8 General Information about Software Development Lifecycle process	47
Table 3-9 General Information about Service Catalogue management process	51
Table 3-10 General Information about Service Level management process	54
Table 3-11 General Information about Configuration management process	58
Table 3-12 General Information about Capacity management process	61
Table 3-13 General Information about IT Service Continuity management process.....	65
Table 3-14 General Information about Availability management process	69
Table 3-15 General Information about Event management process	72
Table 3-16 General Information about Information Security management process	76
Table 3-17 General Information about Supplier management process	81
Table 3-18 General Information about Human Resources management process	84
Table 3-19 General Information about Project management process	88
Table 3-20 General Information about Change management process	91
Table 3-21 General Information about Release and Deployment management process.	97
Table 3-22 General Information about Test management process.....	102
Table 3-23 General Information about Knowledge management process	106
Table 3-24 General Information about Request management process.....	110
Table 3-25 General Information about Incident management process	112
Table 3-26 General Information about Problem management process	116
Table 3-27 General Information about Maturity Level.....	121
Table 3-28 General Information about Quality management process.....	121
Table 4-1 Tables in ITPG database	139
Table 5-1 Processes implemented in IMDB and defined in the proposed model	156

LIST OF FIGURES

Figure 1-1 Relationship between ITIL, COBIT and ISO 17799	4
Figure 2-1 Maturity of Service Management	9
Figure 2-2 Framework / Standards arises from ITIL.....	9
Figure 2-3 Relation between IT Governance and ITSM	10
Figure 2-4 COBIT domains.....	12
Figure 2-5 COBIT processes in domains	12
Figure 2-6 COBIT principle.....	14
Figure 2-7 ITIL Lifecycle.....	15
Figure 2-8 Process areas in each maturity level in CMMI.....	19
Figure 2-9 PDCA model in ISO 27001:2005	20
Figure 3-1 Survey Results: Number of organizations implement standards/frameworks	23
Figure 3-2 Structure of Process defined in the scope of thesis	26
Figure 3-3 Processes based on which frameworks/standards	28
Figure 3-4 Work flow diagram of IT management process	31
Figure 3-5 Sourcing structures	32
Figure 3-6 Tasks that should be done during IT management process	33
Figure 3-7 Flow chart of Service Portfolio management process	36
Figure 3-8 Flow chart of Financial management process	40
Figure 3-9 Flow chart of Risk management process	45
Figure 3-10 Flow chart of Software Development Life cycle process.....	49
Figure 3-11 Flow chart of Service Catalogue management process	52
Figure 3-12 Flow chart of Service Level management process	56
Figure 3-13 Flow chart of Configuration management process.....	59
Figure 3-14 Flow chart of Capacity management process	63
Figure 3-15 Flow chart of IT Service Continuity management process	66
Figure 3-16 Flow chart of Availability management process	70
Figure 3-17 Flow chart of Event management process	73
Figure 3-18 Flow chart of Information Security management process	78
Figure 3-19 Flow chart of Supplier management process.....	83
Figure 3-20 Flow chart of Project management process	89

Figure 3-21 Flow chart of Change management process	93
Figure 3-22 Change Authorization Model	94
Figure 3-23 Flow chart of Release and Deployment management process	99
Figure 3-24 Flow chart of Test management process	103
Figure 3-25 Flow chart of Knowledge management process	108
Figure 3-26 Flow chart of Request management process	111
Figure 3-27 Flow chart of Incident management process	114
Figure 3-28 Flow chart of Problem management process	117
Figure 3-29 Deming cycle	120
Figure 3-30 Activities while improving services	125
Figure 3-31 Flow chart of Service Desk	129
Figure 4-1 ITP Guide Modules	140
Figure 4-2 Use case diagram of ITPG	140
Figure 4-3 Login activity diagram	141
Figure 4-4 Introduction operations activity diagram	142
Figure 4-5 IT Processes Guide Activity Diagram	143
Figure 4-6 View process policies activity diagram	143
Figure 4-7 View process information activity diagram	144
Figure 4-8 View process activities activity diagram	144
Figure 4-9 View Alignment activity diagram	145
Figure 4-10 Manage process information activity diagram	146
Figure 4-11 Manage process general information activity diagram	146
Figure 4-12 Manage process information activity diagram	147
Figure 4-13 Manage process diagrams activity diagram	148
Figure 4-14 An example of page that defining process	149
Figure 4-15 An example of page that defining definition of process	150
Figure 4-16 An example of page that defining role of process	151
Figure 4-17 An example of page defines responsibility of selected role of process	151
Figure 4-18 An example of page that uploading flow chart of process	152
Figure 4-19 An example of page that showing existing processes	152
Figure 4-20 An example of page that showing responsibility of selected role	153
Figure 4-21 An example of page that showing flow chart of selected process	153

LIST OF ABBREVIATIONS

AI	: Acquire and Implement
AMIS	: Availability Management Information System
BIA	: Business Impact Analysis
BS	: British Standards
CFIA	: Component Failure Impact Analysis
CI	: Configuration Item
CMDB	: Configuration Management Data Base
CMMI	: Capability Maturity Model Integration
CMS	: Configuration Management System
COBIT	: Control Objectives for Information and related Technology
CSF	: Critical Success Factors
CSI	: Continual Service Improvement
DS	: Deliver and Support
FDIS	: Final Draft International Standard
FTA	: Fault Tree Analysis
HP ITSM	: Hewlett Packard IT Service Management
IEC	: International Electrotechnical Commission

IS	: Information Systems
ISACA	: Information Systems Audit and Control Association
ISACF	: Information Systems Audit and Control Foundation
ISMS	: Information Security Management System
ISO	: International Organization for Standardization
ISO/IEC27001	: Information technology – Security techniques – Code of practice for information security management
ISP	: Information Security Policy
IT	: Information Technology
ITGI	: IT Governance Institute
ITGI	: IT Governance Institute
ITIL	: Information Technology Infrastructure Library
ITPG	: IT Processes Guide
ITSCM	: IT Service Continuity Management
ITSM	: IT Service Management
KEDB	: Known Error Data Base
KPI	: Key Performance Indicator
ME	: Monitor and Evaluate
ML	: Maturity Level
MOF	: Microsoft Office Framework
MTBF	: Mean Time between Failures
MTBSI	: Mean Time between Service Incidents
MTRS	: Mean Time Between to Restore Service

NPV	: Net Present Value
OGC	: Office of Government Commerce
OLA	: Operational Level Agreements
PDCA	: Plan-Do-Check-Act
PO	: Plan and Organize
PRINCE2	: Projects in Controlled Environment
PSO	: Projected Service Outage
RFC	: Request for Change
ROI	: Return on Investment
SAS70	: Statement of Auditing Standards No.70
SCD	: Supplier and Contracts Database
SCM	: Service Catalogue Management
SDP	: Service Design Plan
SEI	: Software Engineering Institute
SIP	: Service Improvement Plan
SKMS	: Service Knowledge Management System
SLA	: Service Level Agreement
SLM	: Service Level Management
SLR	: Service Level Requirements
SOX	: Sarbanes-Oxley Act
SPOC	: Single Point of Contact
SPOF	: Single Point of Failure
TSO	: The Stationary Office

UK : United Kingdom

VBF : Vital Business

CHAPTER 1

INTRODUCTION

1.1 Background

As a consequence of the fact that information technologies strategically differentiate organizations, structuring and managing IT activities has become one of the main focuses of the organizations [1]. In addition, IT assets (computer hardware, software, telecommunications facilities and human knowledge capital) have become essential for effective organizational management as they provide great value to business [2], [3]. To be successful in business, IT infrastructure should be effectively managed in the organization because of the fact that “IT is now at the core of most organizations” to execute strategy [5]. The practice of IT governance has emerged as a discipline to enable organizations better managing IT assets and so investments. In addition to this, to enable effective management IT, a great number of IT governance standards/frameworks are emerged, including ITIL (Information Technology Infrastructure Library), COBIT (Control Objectives for Information and Related Technology), ASL (Application Services Library), Six Sigma, CMM/CMMI, IT Service CMM, SAS70, ISO 17799, SOX, SysTrust, PRINCE2 [6].

These frameworks cover different aspects of IT and not a single one is adequate to provide effective IT Governance. To manage IT as a whole efficiently, different models

should be applied together [5]. However, implementing different models into an organization is considerable difficult and requires more expertise.

These frameworks have been translated to a few different languages. Since, Turkish has not been in these translated languages, this issue has become one of the reasons that prevent organizations in Turkey adapting these frameworks easily and effectively.

To conclude, IT governance is an important discipline that has to be practiced by all organizations utilizing IT assets for their business. Due to, there exist many frameworks to aid organization in their IT operations. Since they are supplementary rather than comparative, they should be implemented together. However, jointly application of these frameworks is rather difficult. Also, Turkish resource about the IT governance concept and the well known frameworks are also needed for Turkish organizations to manage IT effectively.

1.2 Problem Statement

Organizations applying IT governance discipline earn at least 20% higher return on assets than those with weak IT Governance practice [7]. Thus, IT governance is essential for organizations independent of the size. However, effectively governing IT is not as easy as considered. The meaning of IT governance is unclear for most of the organizations due to the disparate terms and quite distinct definitions of IT governance [8] in research area. IT governance concept will be explained detail in Chapter 2.1.

There is high increasing not only in the usage of standards/frameworks individually but also in implementing several framework/standards simultaneously [9]. Since, many of the existing frameworks in IT Governance are supplementary and each framework has focused on different areas, a mix-and-match approach is often taken by organization that aim is to govern IT effectively [5]. But mix-and-match approach for organizations is more difficult than considered. Hayden stated that implementing multiple frameworks

separately needs more cost and effort in the organization's compliance initiatives due to redundancy duplication derived from similarities between various frameworks [10].

Well known frameworks/standards that supplement each other such as COBIT, ITIL, CMMI and ISO 27001 all provide IT processes to experts to achieve the implementation of these frameworks/standards which shows that they are process based. Due to the fact that process management plays an important role within the implementation of them.

While implementing effective IT processes, well known frameworks COBIT and ITIL that support them [11] are used mostly.

Two most important and common frameworks ITIL and COBIT have existed for more than 10 years are used by thousands of organizations of all sizes and sponsored by very well-respected organizations ISACA and ITGI respectively. However COBIT and ITIL are very different in terms of orientation and definition. On account of this, ITIL and COBIT is more complementary rather than competitive. [12]

Based on the experience on five Australian organizations, implementing ITIL means the transforming IT service management to gather vital benefits such as more control on testing and changes, more predictable infrastructure, improved consultation within organization, reduced server failures, documented and consistent IT service management processes and compatible recording of incidents [13]. Most of organizations thought that they gain much more value by implementing of ITIL that is the reason why processes are based on it in the scope of thesis.

With the growing technology, Information security has become an important issue in IT Governance and fundamental aspect of IT governance is to protect the information on which business depends [14] [15]. However, also information security is essentially

managerial issue rather than a technical one. [15]. Thereof it should be included in IT governance processes as seen in ITIL and COBIT.

There is an increase in the certification in ISO 27001:2005. The reasons are the followings [15];

- The threats to information becomes widespread
- Increasing range of regulatory and statutory requirements for information protection

To sum up, As Hardy pointed out, unification of IT governance frameworks should include COBIT, ITIL and ISO 27001 which have become widely popular around the world [17]. In addition, Solms underlined the benefits of integrated application of COBIT, which provides wider reference and integrated platform, and ISO 17799, which provides more detailed guideline about Information security [18]. In addition to all these, CMMI, having very high level mature and well known framework in Turkey is complementary to COBIT and ITIL [19]. COBIT, ITIL and ISO 27001 frameworks meet different needs of organizations as seen in the Figure 1.2 [20].

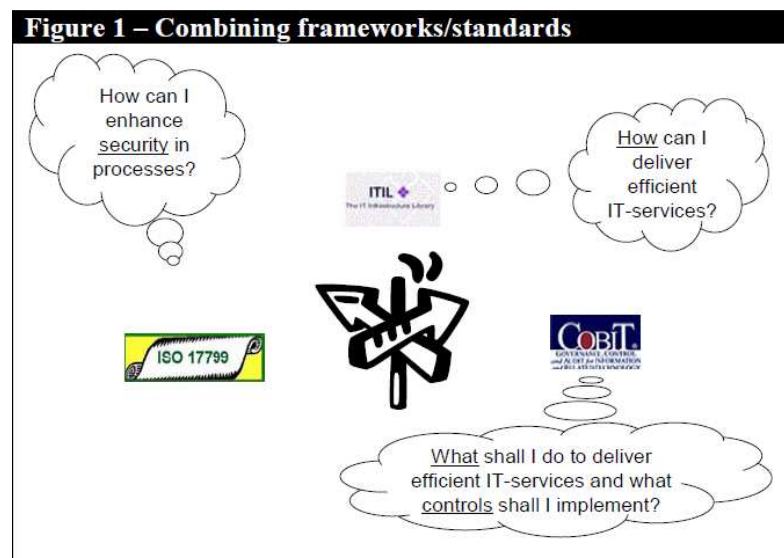


Figure 1-1 Relationship between ITIL, COBIT and ISO 17799

As a result, there is a need for unification of processes offered by well known process based frameworks or standards for the organization to reduce duplication and effort while implementing these frameworks separately.

Besides, qualitative analysis with informal methods is done. Three experts working in Central Bank of the Republic of Turkey, Banking Regulation and Supervision Agency and Social Security Institution were interviewed face to face with the questions in Appendix N. The results of interview show that there is a Turkish resource need about the IT management concept due to the lack of Turkish resources in literature. This causes that systematic study or central coordination mechanism against to IT governance over organizations is unavailable yet in Turkey [21]. Although, ISO 27001 has been translated to Turkish, COBIT and ITIL has not been yet.

1.3 Objective of Thesis

1. The objectives of this study is to establish a unified IT process model;
 - To cover both COBIT and ITIL requirements.
 - To reduce the duplicate effort of implementing different standards separately.
 - To include CMMI level two requirements into the processes in order to establish a foundation for application of higher maturity CMMI levels.
 - To define a management framework of ISO 27001 this can be extended to technical aspects of standard.
2. Another major objective of thesis is to map the unified process models with the requirements of COBIT and ITIL in order to show the alignment with these two widely used frameworks.
3. The last objective of this study is to provide dynamic web based application;

- To provide knowledge bank foundation this contains processes and their attributes in Turkish.
- To provide profile pages for organizations to manage, trace and reach their processes' easily within the organization.
- To increase the number of organizations that implement IT processes within the Turkish organizations especially for public organizations whatever the size.

1.4 Outline of Thesis

In chapter 1, an introduction of the thesis is given and background, problem statement and objectives are explained.

In chapter 2, besides what IT governance and IT service management is, general information about the common standards used for IT management which our methodology based on is explained.

Chapter 3 provides the need of the unification of two main standard/framework used commonly in recent years. After all, all processes are explained in detail and every processes and their attributes are aligned with used standard/framework double sided.

In chapter 4, general information about IT Processes Guide (ITPG) is mentioned. Design of IT Processes Guide database and software is explained in main two parts respectively. And lastly, sample representation of the usage of ITPG is provided.

Chapter 5 includes the justification of the proposed solution in a very well known organization in Ankara in Turkey. Firstly, processes composed in that organization and created in the scope of thesis are compared and differences are explained. Later, consequences of the implementation of proposed solution are given.

Chapter 6 explains conclusion of the study and includes future works for proposed solution.

CHAPTER 2

FOUNDATIONS OF IT GOVERNANCE AND RELATED RESEARCH

This chapter introduces basic concepts related to the Information Technology (IT) Governance and IT Service Management. It provides firstly meaningfully definition of IT governance and service management, mentions need of the IT governance and frameworks and finally introduces the major framework types used in world as the IT governance/management frameworks and standards.

2.1 What is IT Governance and IT Service Management

“IT Governance” term is first used by Loh and Venkatraman in 1992 and Henderson and Venkatraman in 1993 but in the academic literature in the late 1990s had been seen first by Brown in 1997 and Sambamurthy and Zmud in 1999 as the notion of “IS Governance Frameworks” and then later to “IT Governance Frameworks” in their papers [8].

The definition of IT Governance offered by the IT Governance Institute (ITGI), the body that created COBIT is as the following; “IT Governance is the responsibility of executives and the board of directors and consists of leadership, organizational structures and processes that ensure that the enterprise’s IT sustains and extends the organization’s strategies and objectives” [22].

Today, with growing technology lots of companies of the business use Information Technology (IT) while delivering services to their customers. “%87 of business now identifies themselves as ‘highly dependent on electronic information and the systems that process it.’ [14]. According to the survey done by ITGI in 2006 [24] shows that IT is vital in terms of the delivery of the business strategy and also participants thought that better IT governance practices improve the governance of IT resources. As a result, IT governance plays an important role for the organizations that use IT. However, in recent years, there is a huge failure of IT investments [23].

On account of this, IT governance has been thought as an important issue that has to be managed to improve corporate success by deploying information through technology application [25] and IT governance has become a very important issue for the companies of the business in the world. It will continue growth of importance for companies. In fact, in the future, it will become even larger factor [26]. The position of IT in corporate governance is increasingly become clearer because of that information technology has become spreading throughout and supporting every aspect of the organization [15].

There exist five domain for IT governance; IT Strategic Alignment, IT Value Delivery, IT Resource Management, IT Risk Management and IT Performance Management. The relation between IT strategy and business goals is the key for IT governance’s effective and efficiency [27].

On the other hand, IT service management (ITSM) is defined as “a set of specialized organizational capabilities for providing value to customers in the form of services.”[28] IT Service Management is emerged first in the middle of 1980s. Evaluation of IT service management is given in the following Figure 2.1 [29];

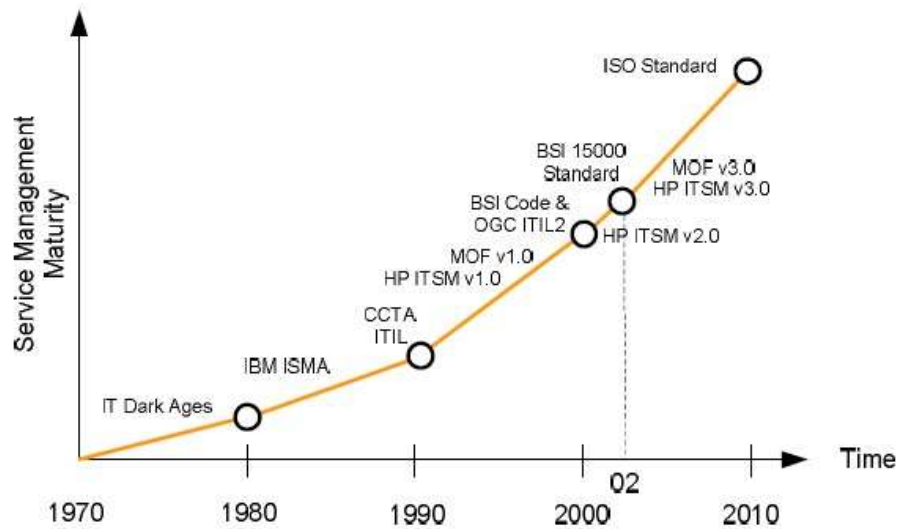


Figure 2-1 Maturity of Service Management

Relation between the recent standards/frameworks shown in Figure 2-1 of IT service management is seen in the following figure [29];

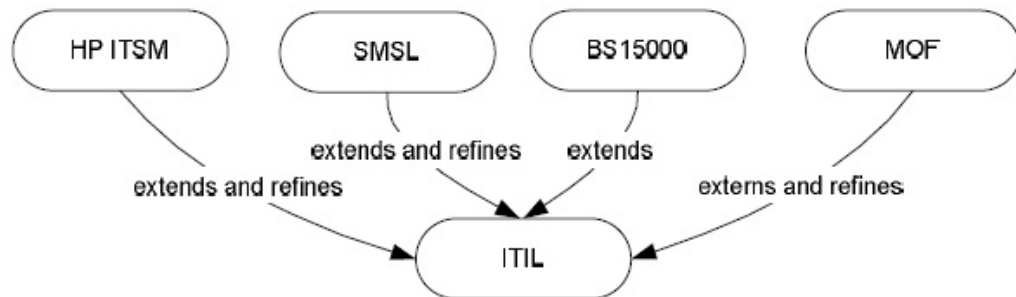


Figure 2-2 Framework / Standards arises from ITIL

As seen in the figure, all frameworks/standards related to ITSM arise from ITIL. Because of the reason ITIL can be seen as the de facto standard ITSM [29]. There is a strong relationship between IT governance and ITSM as shown in the following figure [29]. IT governance and IT service management serves two different aims. IT governance is related to “what” the IT organization should achieve, however, IT service

management is related to “how” the IT organization will achieve [29]. Also, the relationship between the two critical terms is figured like in the following figure [29];

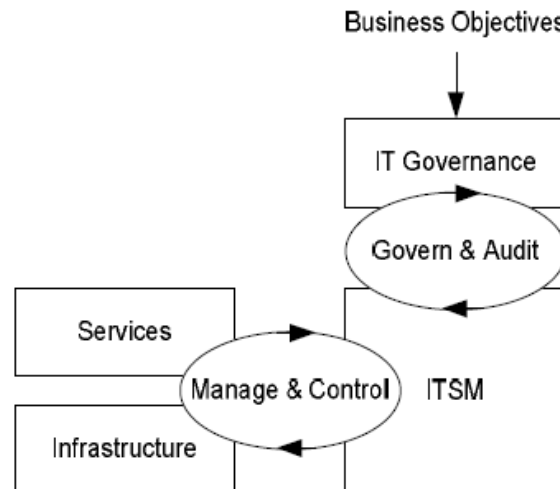


Figure 2-3 Relation between IT Governance and ITSM

According to the IT Forum Conference by Microsoft 2004, studies done on recently shows that by applying IT service management principles, organizations could achieve %48 percent reduction in cost. In addition to this, Forrester claims that revenue of large companies adopting ITIL, excess 1 billion dollars increased from %13 to %20 in 2006 [30].

Today, in world there exist lots of frameworks used for companies that use IT to be more successful such as COBIT, ITIL, and ISO27001. These standard/frameworks which are used for proposed solution will be explained in the following chapters in detail. All these processes and standard are process based.

2.2 Framework Types Used

This chapter consists of four major sections. First section introduces the COBIT framework structure. Second section presents ITIL lifecycle and mentions about its

major five publishing briefly. Third section explains CMMI usage and meaning which is different from COBIT and ITIL totally but it is complementary of them in terms of its types and process areas. ISO 27001 is explained in chapter four. Last chapter introduces the unification of these processes of frameworks done up to now.

2.2.1 COBIT

Control Objectives for Information and Related Technology (COBIT) is an open standard to provide controlling over Information Technology improved by IT Governance Institute (ITGI) as a part of the Information Systems Audit and Control Association (ISACA). The tool set facilitates IT governance, defined as “a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise’s goals by adding value while balancing risk versus return over IT and its processes” [23].

Main objective of the COBIT is the development of clear policies and good practices for security and control in IT from the business perspectives. COBIT provides the alignment of the IT with the business objectives i.e. Control objectives in COBIT links to business objectives clearly and distinctly [31]. COBIT is strong in IT controls and metrics, but it does not say how results in difficulties of implementation of processes.

COBIT framework is composed of domains and high level control objectives or processes. It provides four interrelated domains shown in figure 1 named as Plan and Organize, Acquire and Implement, Deliver and Support and Monitor and Evaluate and thirty four processes.

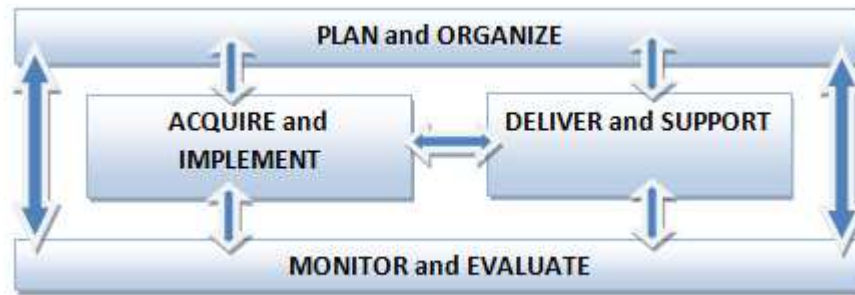


Figure 2-4 COBIT domains

Each domain has processes shown in the following figure;

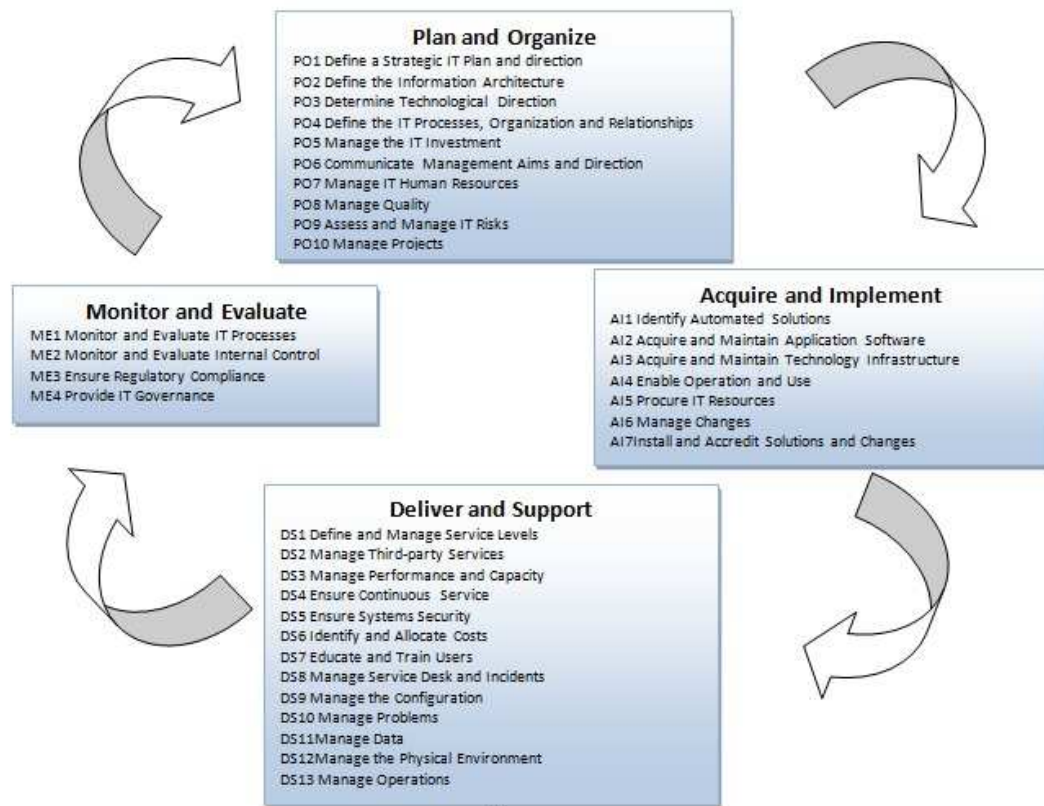


Figure 2-5 COBIT processes in domains

Each process consists of description of it together with key goals and metrics and relationship with the IT governance focus areas (Strategic Alignment, Value Delivery, Risk Management, Resource Management and Performance Measurement) and IT

resources (Applications, Information, Infrastructure and People), audit guidelines (totally 318 control objectives), management guidelines and maturity model.

Management guidelines includes the inputs and outputs of the processes, RACI (identifies which stakeholder is Responsible, Accountable, Consultant and Informed about certain activities) chart and goals and metrics in terms of the IT, process and activities.

Maturity Models show the IT Organization maturity level with regard to IT processes in today. Maturity level is scaled from 0 to 5.

COBIT provides the following enterprises to understand the risks and benefits of IT;

- Aligning IT strategy with the business strategy
- IT risks which had been met to the investors and shareholders
- Cascading IT strategy and goals and activities
- Value from IT investment
- Organizational structures that implements the IT strategy and goals
- Constructive relationships and good communication between business and IT and with external parties
- IT performance

COBIT framework provides the business-focused, process-oriented, control-based and measurement-driven main characteristic to respond to the need for IT governance framework.

Since alignment of IT strategy with business strategy is very important in IT governance, business orientation is the main theme of COBIT framework. It is not only designed for IT service providers or others related to the IT service, it also behaves as guidance for management and business process owners. The COBIT framework is based on the following principle; “To provide the information that the enterprise requires to

achieve its objectives, the enterprise needs to invest in and manage and control IT resources using a structured set of processes to provide the services that delivered the required enterprise information.” [22]

This principle is shown in the following figure;

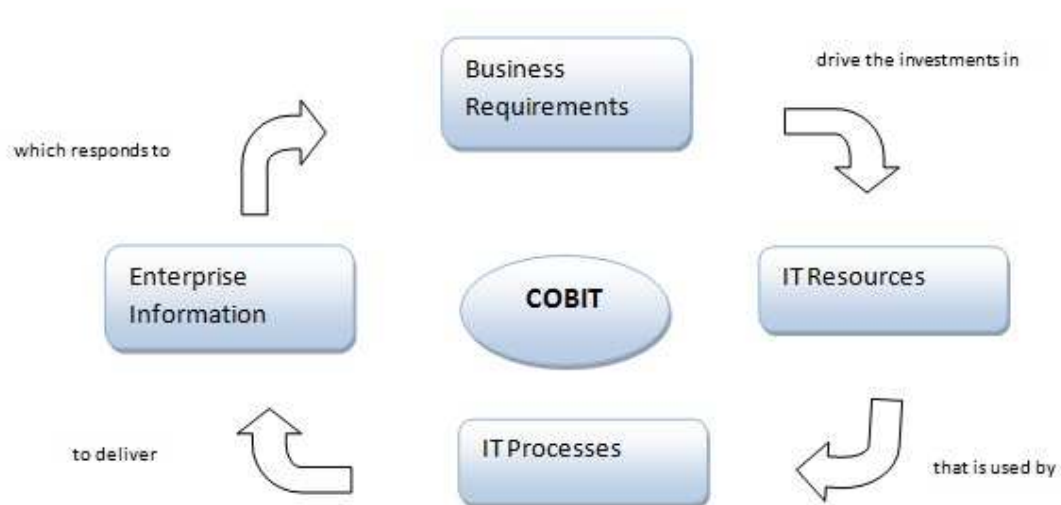


Figure 2-6 COBIT principle

2.2.2 ITIL

In the late 1980s, the UK’s Central Computer and Telecommunications Agency (CCTA) developed IT Infrastructure Library (ITIL) to provide IT service management providing lower cost and better delivery of services [9], [29].

ITIL (IT Infrastructure Library) v3 similar to COBIT provides best practice about Service Management introduced by British government’s Office of Government Commerce (OGC) in and ITIL has become the famous approach to IT service management accepted widely by many organizations since its creation [32]. The definition of the service management introduced by the OGC in ITIL books is given as

the following; “Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services.” [28] As stated in the definition, firstly organization must understand what services are. Again, in ITIL books service definition is given as the following; “A service is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks”. [28]

ITIL has the following components; The ITIL Core and The ITIL Complementary Guidance. ITIL Core is composed of five publications;

1. Service Strategy
2. Service Design
3. Service Transition
4. Service Operation
5. Continual Service Improvement

All publications defined in ITIL core is in the form of a lifecycle.

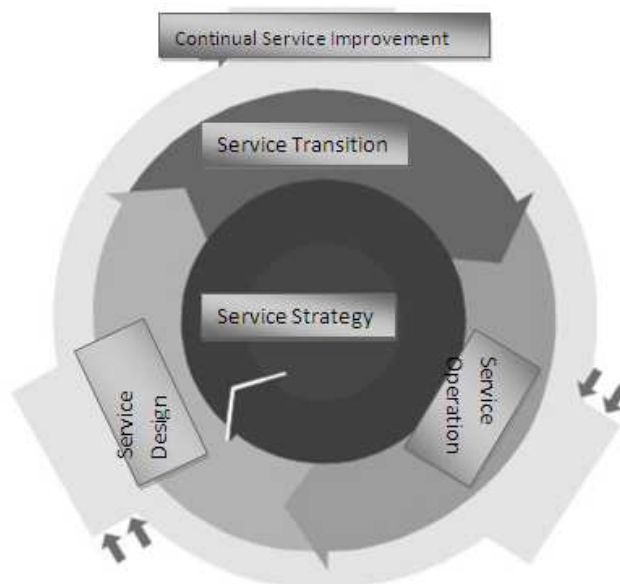


Figure 2-7 ITIL Lifecycle

These core five publications are the starting point for ITIL V3. The content of these books can be enhanced by the complementary guidance which can be knowledge and skills, specialty topics, templates, governance methods, standards alignment, executive introduction, study aids, qualifications, quick wins, scalability and update service.

In each core publications, ITIL defines the processes in detail, provides good practices and give recommendations about IT Service Management. The processes described in ITIL V3 follow a similar structure:

- Purpose, goals and objective
- Scope
- Value to the business
- Policies, principles and basic concepts
- Process activities, methods and techniques
- Triggers, inputs, outputs and interfaces
- Key performance indicators (KPIs) /metrics
- Challenges, critical success factors (CSFs) and risks

With the use of ITIL, customer satisfaction, quality of services and constructive contribution to business will increase. Customer satisfaction in addition to operational performance increases with the increasing use of activities in ITIL framework [33].

2.2.2.1 Service Strategy

Service strategy is a kind of guidance that mentions about how to design, develop and implement service management as a strategic asset in addition to organizational capability [28]. In the process and activities in Service strategy, Business goals and contribution of service providers to services to achieve the business goals are defined

[34]. Financial Management, Service Portfolio Management, Demand Management are the key processes described in Service Strategy [32].

2.2.2.2 Service Design

Service Design role is defined as “The design of appropriate and innovative IT services, including their architectures, processes, policies and documentation, to meet current and future agreed business requirements.” [32], [35]. Service Design is also a guidance that explains how to design and development of services and service management processes not only limited to new services but also changing services [35]. Service Catalogue Management, Service Level Management, Capacity Management, Availability Management, IT Service Continuity Management, Information Security Management and Supplier Management are the processes defined in Service Design [32], [35].

2.2.2.3 Service Transition

Service Transition provides guidance on how to transition new or changed services into live environment by developing and improving capabilities [36]. Transition Planning and Support, Service Asset and Configuration Management, Change Management, Release and Deployment management, Service Validation and Testing and Knowledge Management are the processes defined in Service Transition publishing.

2.2.2.4 Service Operation

Service Operation provides guidance on how to operate service delivery and support in terms of achieving effectiveness and efficiency to ensure that service user and service provider get value [37]. Event Management, Incident Management, Request Fulfillment, Problem Management and Access Management are the processes defined in that book.

Also, service desk with application management, operation management and Infrastructure management is covered in that book as an activity.

2.2.2.5 Continual Service Improvement

This book provides guidance on how to create and maintain value by better design and operation of services [38]. Closed loop feedback system based on Deming cycle (Plan-Do-Check-Act) is used.

2.2.3 CMMI

CMMI is firstly release from Software Engineering Institute (SEI) as software capability maturity model (CMM) version 1.0 at Carnegie Mellon University to define principles about software development process maturity. Defined software development process improves the success of the software projects by increasing quality and reducing risks [39]. In 1991 SEI firstly released capability maturity model integration (CMMI). Now Version of CMMI is 1.2. As Borland state that CMMI is the complementary of ITIL framework which scope of CMMI is the development of the system whereas scope of the ITIL is the operation of the system [40].

CMMI is composed of 5 maturity levels; Level 1 – Initial; Level 2 – Managed; Level 3 – Defined; Level 4 – Quantitatively Managed; Level 5 – Optimizing.

The following figure shows process areas in each maturity level [39].

Process areas in CMMI-SW/SE staged representation		
Maturity level (ML)	Focus	Process area
ML 5: Optimizing	Continuous process improvement	Organization innovation and deployment (OID) Causal analysis and resolution (CAR)
ML 4: Quantitatively managed	Quantitative management	Organization process performance (OPP) Quantitative project management (QPM)
ML 3: Defined	Process standardization	Requirements development (RD) Technical solution (TS) Product integrated (PI) Verification (VER) Validation (VAL) Organizational process focus (OPF) Organizational process definition (OPD) Organizational training (OT) Integrated project management (IPM) Risk management (RSKM) Decision analysis and resolution (DAR)
ML 2: Managed	Basic project management	Requirements management (REQM) Project planning (PP) Project monitoring and control (PMC) Supplier agreement management (SAM) Measurement and analysis (MA) Process and product quality assurance (PPQA) Configuration management (CM)
ML 1: Initial	ad hoc process	None of process areas

Figure 2-8 Process areas in each maturity level in CMMI

2.2.4 ISO 27001

All organization depends on IT resources not only for their survival but also their growth and competition. Because of the fact that all resources must be protected according to the guidelines found in BS 7779 and COBIT [41] ITIL has also take consideration for Information Security in Service Design publications [35]. The world was introduced to the formal concept of an information system (ISMS) during the 1990s with the development and introduction of the British Standard – BS-7779 [16]. The information security standards are essential starting point for any organization that is commencing an information security project [15]. BS 7779 was finally replaced in October 2005 with ISO 27001:2005 by the Final Draft International Standard (FDIS) [42]. ISO/IEC FDIS 27001 is an international standard stands for Information technology- Security techniques – Information security Management systems – Requirements.

ISO 27001 defines a Information Security Management System(ISMS) of which the design is influenced by the organization needs and security requirements. Information Security Management can be defined as a management system used for establishing and maintaining a secure information environment [43].

The aim of ISO 27001 is to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving ISMS. Like COBIT and ITIL, ISO 27001 also has a process based approach of management of security.

The International Standard adopts the “Plan-Do-Check-Act” PDCA process model which is applied to all ISMS processes [44], [45].

In the following figure PDCA model is shown;



Figure 2-9 PDCA model in ISO 27001:2005

2.3 Unification of IT Management Processes in Literature

Although, academic society and IT organizations realized that most of frameworks especially COBIT and ITIL should be implemented together, there is no study on that subject producing a new framework containing both of their requirements.

Firstly, ISACA produces a report based on aligning COBIT and ITIL but does not produce new processes only shows relationship between the ITIL chapters and COBIT control objectives. But this document is quite important document referenced for processes created during the preparation of this thesis.

There is an another study which produce a new framework for only one process “Information security management” by unifying ITIL Security management and COBIT DS5(Ensure System Security) Control objective [46].

Most of organizations especially consulting firms and software organizations produce their own processes based on ITIL and COBIT, such as IBM Tivoli, HP ITSM and Alcyone Consulting Firm, but not totally depends on them and not for academic study. For this reason, They are not explained in the scope of this study.

CHAPTER 3

PROBLEM DEFINITION AND OUR PROPOSED SOLUTION

3.1 Method for Construction Processes

Implementing, managing and supporting IT processes and services effectively results in more success, less downtime hours, less failures, excessive revenue, scarce cost, good communication and realization of business objectives [35]. Therefore, processes defined both in COBIT and ITIL are combined to meet requirements of both to achieve them and to provide the above defined advantages. This thesis is based on processes necessary for IT organizations.

According to managers, IT service management and IT governance frameworks are not separated, they should be combined to provide powerful IT governance and best practice for service management [47], [29], [9]. Recently, organizations adopt multiple frameworks COBIT and ITIL at the same time [9]. Organization are compulsory to implement COBIT to put their ITIL program into context of a wider governance because ITIL is not a complete approach although it provides good documentation of IT processes [9].

According the survey at itSMF done on total 500 delegates, 110 responses were returned, that most organizations start to implement more than one framework/standard

together. This survey shows that, all responses organizations implement ITIL, also adapt to other frameworks [9];

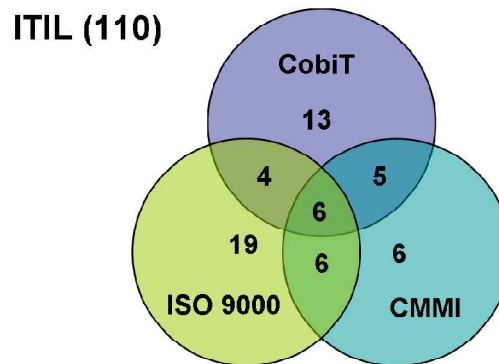


Figure 3-1 Survey Results: Number of organizations implement standards/frameworks

However, implementation of all these frameworks results in important issues which are interrelationship and process overlaps; for example, configuration management is handled by both CMMI and ITIL. Thus, overall plan is adopted rather than separate plan for each framework process adoption [9].

While defining the processes during thesis, ITIL is based and COBIT processes are added over them. Because, ITIL is strong in processes and explains the process flows (i.e. the way of doing job) although COBIT is composed of processes, it does not contain steps and tasks to realize processes [48]. It focuses on what the organization should do but do not explain how it should be done. On the contrary, ITIL defines how processes are achieved by giving flow charts [49].

To sum up, since the aim of thesis is to provide implementation of processes easily by giving not only what but also **how** to achieve, ITIL processes are based. The reason why COBIT is also handled is that the COBIT extensive perspective i.e. some processes handled by COBIT but not by ITIL, i.e. ITIL has many deficiencies with respect to COBIT, for example, ITIL focuses on operations but ignores development/solutions [50].

Furthermore, from the implementation view, ITIL is the easier standard to be implemented. Because, ITIL could be implemented partially and still not have impact on performance. For example, if IT department lack of budget and he could choose to implement IT Service Delivery layer only, and the next year he will try to implement IT Release Management or IT Problem Management. However COBIT is quite difficult to be implemented partially, since it should see a process in bigger view first before they could be implemented partially. [51]

Troy DuMoulin managing consultant at Pink Elephant stated that most of the frameworks have ITIL at their core such as, 45-50% of control objectives of COBIT are covered with in ITIL [52].

To sum up, since implementation of ITIL is easier than the COBIT, ITIL is the core of COBIT and ITIL mentions “how” not only what, in this thesis, the processes are similar to ITIL and since COBIT contains wide set of resources including all the information that organizations need while adopting IT governance and control framework [53], the processes are enriched by COBIT’s control objectives.

Since security has become the important process that has to be handled, ISO/IEC27001:2005 management document is covered to define information security management process flow with the ITIL and COBIT. ISO 27001 management structure i.e. Plan (establishing), Do (Implementing and operating), Check (Monitoring and Reviewing) and Act (Maintaining and improving) is taken in the consideration in information security management process as in ITIL and ISO 27001.

In the following Table 3-1, the comparisons of three framework/standards are given [51];

Table 3-1 Comparison of COBIT, ITIL and ISO 27001

AREA	COBIT	ITIL	ISO27001
Function	Mapping IT Process	Mapping IT Service Level Management	Information Security Framework
Area	4 Process and 34 Domain	9 Process	10 Domain
Issuer	ISACA	OGC	ISO Board
Implementation	Information System Audit	Manage Service Level	Compliance to security standard
Consultant	Accounting Firm, IT Consulting Firm	IT Consulting firm	IT Consulting firm, Security Firm, Network Consultant

While forming processes, ITIL V3 and COBIT 4.1 are considered basically by taking unification of their processes. During taking unification of ITIL processes with COBIT processes, the document “Mapping of ITIL V3 with COBIT V4.1” produced by ISACA [54] is based especially to detect the overlapping of processes and intersection of them. This document includes the alignment of COBIT and ITIL and ITIL-COBIT bidirectional. It also shows the level of how much the control objectives of COBIT processes are covered at COBIT-ITIL alignment part in five levels are shown in table 3.2.

Table 3-2 Coverage types between COBIT and ITIL [54]

Coverage Type	Definition
E	Exceeded
C	Complete coverage
A+	Many aspects addressed
A	Some aspects addressed
A-	A few aspects addressed
N/A	Not addressed

Using these level also helps to understand the whether ITIL processes are enough to meet the control objectives or not.

Not all processes are emerged only by COBIT and ITIL. There is a exception case in Knowledge Management process. Knowledge management process is divided into three part; Knowledge Management Strategy, Knowledge Transfer and Data and Information Management [55]. Because of this reason and to minimize the number of processes and functions to prevent complexity, although data and information management is considered separated process in COBIT and function in ITIL from Knowledge Management, in the thesis' scope, data and information management is handled in Knowledge Management process.

3.2 Purpose and Scope of Proposed Solution

The details of COBIT and ITIL are given in section 2, form this thesis' approach. In this approach is to provide IT service management processes are aligned both COBIT and ITIL, implemented by a great deal of organizations. Because of the deficiency in Turkish source about the IT service management, another purpose of this approach is to provide a web based application prepared in Turkish for Turkish Organizations.

The structure of processes prepared in the scope of thesis is suitable with ITIL processes. Each process contains definition, purpose, scope, business value, activities & tasks (if applicable, most of them are figured out as flow charts), inputs/outputs, roles and metrics.

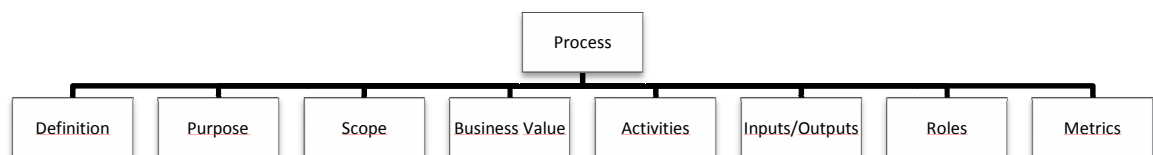


Figure 3-2 Structure of Process defined in the scope of thesis

Definitions of the terms used in defining processes and functions are also given in Section 3.2.1. In addition to this, the alignment of the processes with COBIT and ITIL are given in Appendix J, K, L and M.

Since, the processes in the scope of the thesis is prepared by using the process definition defined in ITIL books and given in Section 3.2.1, some set of functions like service desk or application management is not stated as process. The characteristic of process stated in ITIL Service Operation book are measurable, specific results, customers and responds to specific events. Since there is no chance to count results of service desk like “how many Service Desks were completed?” service desk can be thought as process on the contrary to COBIT [22], [37].

For this reason, we define four functions explained in Section 3.2.3 which are Service desk, application management, technical management and operational management.

3.2.1 Terms and Definitions

In general, the definitions of the terms used in this recommended IT processes model are provided in this in Appendix I.

3.2.2 Processes

There exist twenty five processes which are covered by three main parts;

- Principles
- General Information
- Flow Chart

General information covers purpose, scope, and value to business, input, outputs, roles, tools, metrics and activities.

If activities and tasks can be figured out by using flow chart, it is stated as flow chart. Otherwise, it is stated in activities row of tables of General Information part as a text. Flow charts are figured out by using “Microsoft Office Visio 2007 Flowchart Shapes (Metric)”. Meaning of the shapes used in flow charts are given in Appendix O.

All processes defined in the scope of thesis are shown in the following figure which states that which processes are based on which framework/standards.

Each color shows the different combination of processes¹. The details of all processes are explained in the following chapters detail and these processes can be documented by using process documentation template in Appendix C.

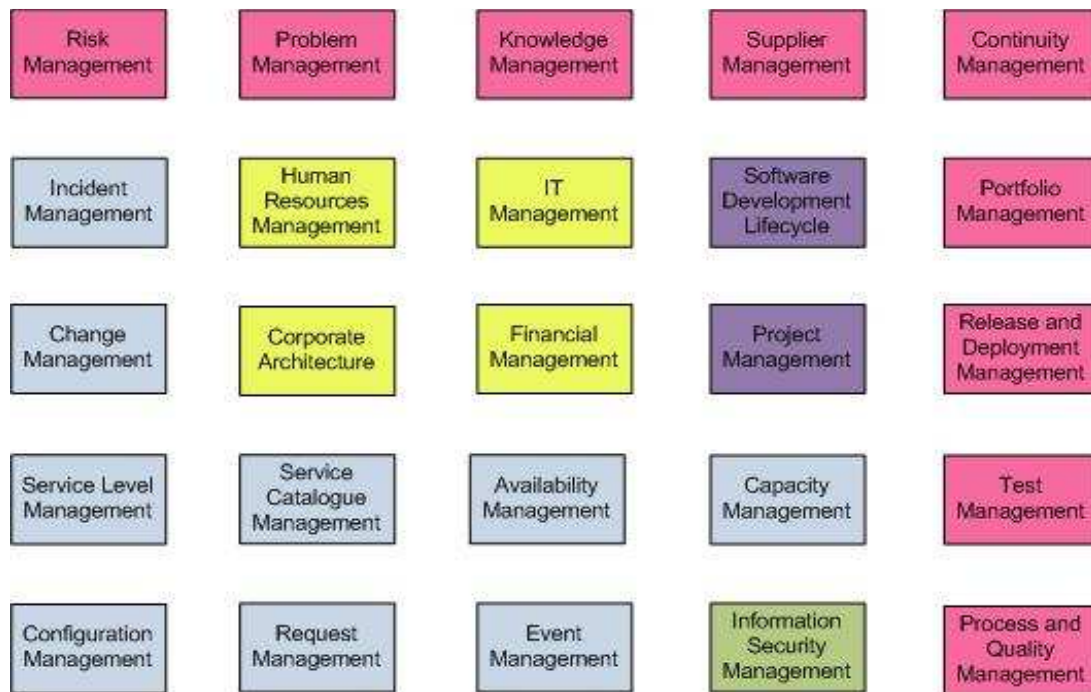


Figure 3-3 Processes based on which frameworks/standards

¹Blue: ITIL based
Yellow: COBIT based
Red: ITIL and COBIT based
Purple: COBIT and CMMI based
Green : COBIT, ITIL and ISO 27001 based

P.1 IT Management

Principles:

1. Define Market
2. Develop Offerings
3. Develop strategic assets
4. Preparing for application

Strategy is crucial for organization performance.

- a. Strategic evaluation
 - i. Which of our services or service varieties are distinctive?
 - ii. Which of our services or service varieties are the most profitable?
 - Etc.
- b. Set targets
- c. Aligning service assets with customer outcomes
- d. Defining critical success factors
- e. Rivalry Analysis
 - i. Entrance level
 - ii. Industry averaging
 - iii. Best practice of industry
- f. Exploring business potential
 - i. Making SWOT analysis
- g. Alignment with customer needs
- h. Expansion and Growth
- i. Differentiation in marketing

Strategic Plan should contain the followings:

- Contribution of IT goals to business strategic goals and related cost and risks
- How IT support investments based on IT, IT services and IT assets
- Procedures of how IT goals are meet, what metrics are used and approval from stakeholders
- Investment/operational budget

- Financial Resources
- Sourcing strategy
- Supplier strategy
- Legal and regulatory requirements

General Information:

Table 3-3 General Information about IT management process

Process ID	P.1
Process	IT Management
Purpose	Defining IT goals to meet current and future business requirements with business and executive managers (Business-IT Alignment)
Scope	Defining IT strategy suitable to current and future business requirements with business and senior managers Understanding of current IT capacity
Values to Business	IT strategy becomes transparent in terms of cost, benefit and risk and conformance with business strategy and requirements
Inputs	Risk Assessments Cost -Benefit Reports Project and Service Portfolio Service Reports / SLRs Business Requirements
Outputs	IT Strategic/Tactical Plan IT Sourcing/Acquisition Strategy Documented roles and responsibilities IT Policies
Roles	IT Committee Business Relationship manager Process and Quality Manager
Metrics	Percent of IT goals defined in IT strategic plan supporting strategic business plan Delay between update of business strategic and tactical plans and IT strategic and tactical plans Involvement of business part into strategic tactical IT plans actively

Flow Chart:

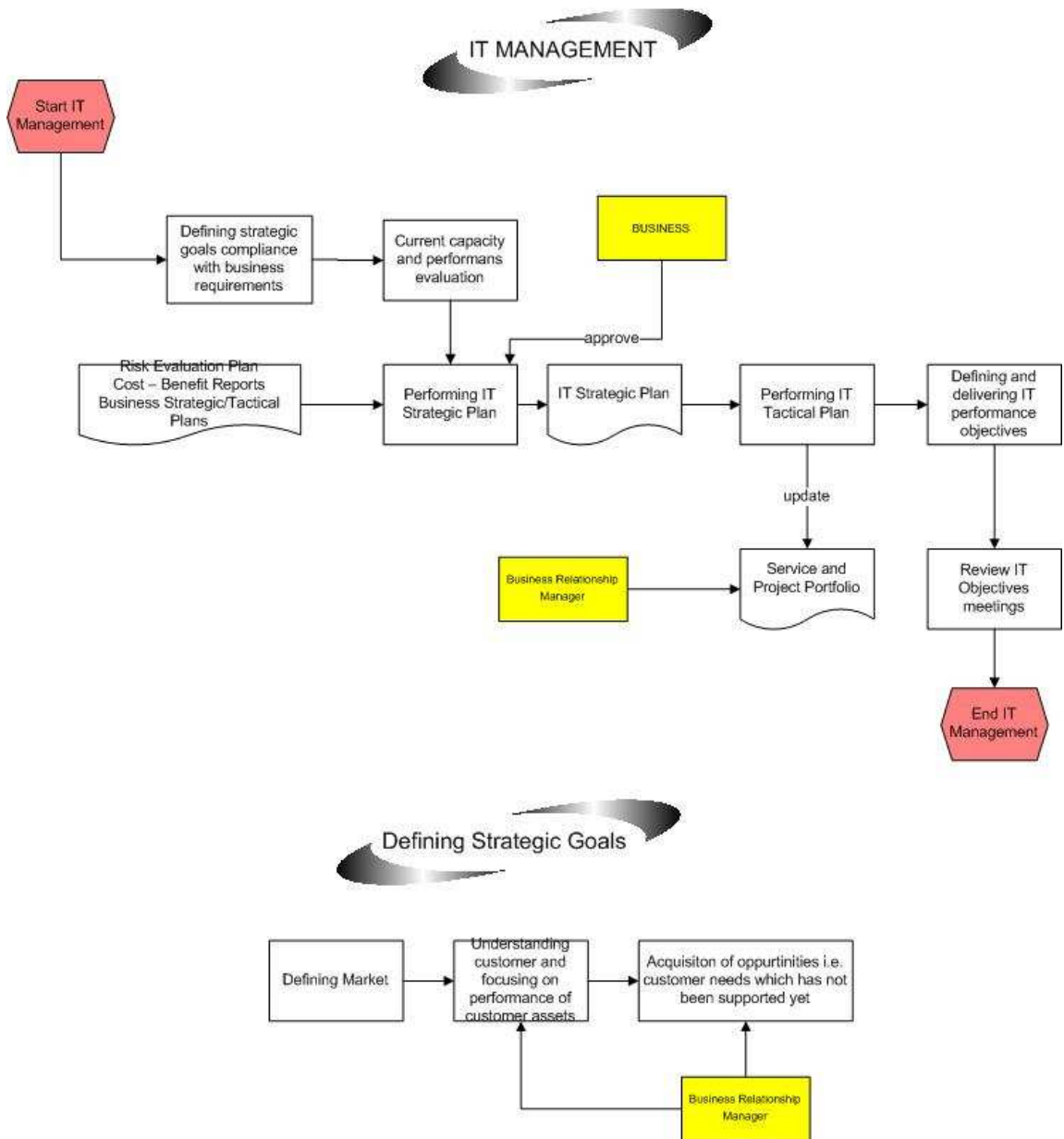


Figure 3-4 Work flow chart of IT management process

In the strategy plan, sourcing strategy is defined according to the sourcing structures.

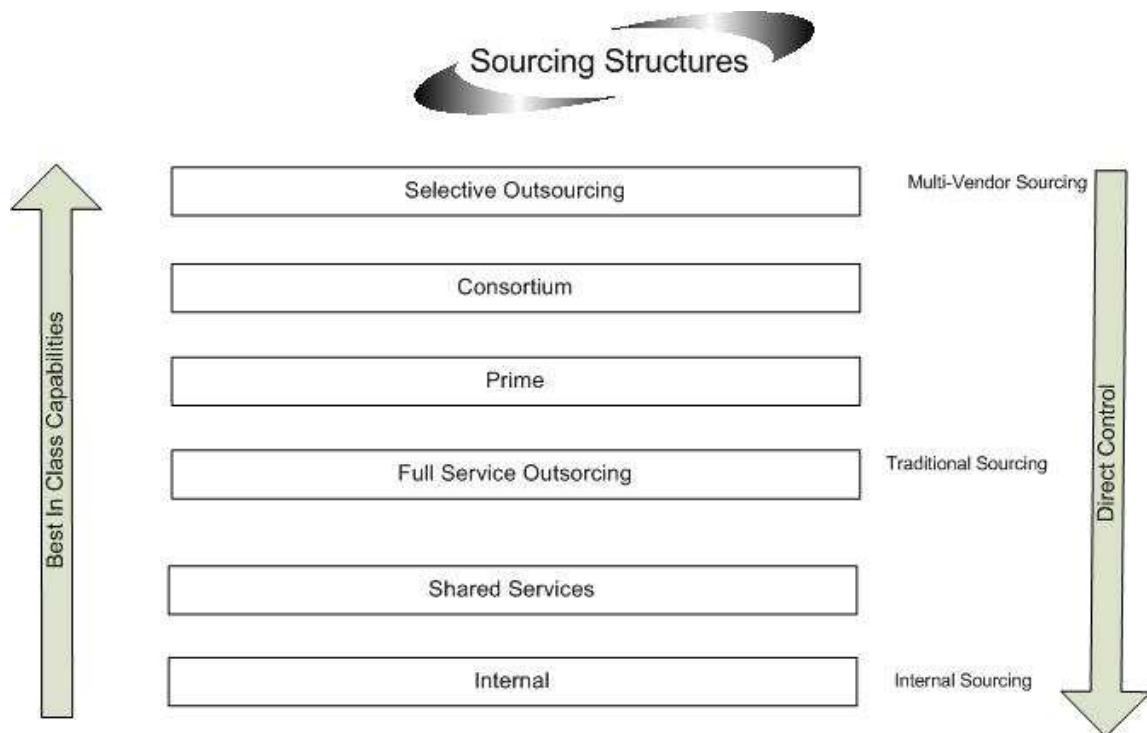


Figure 3-5 Sourcing structures

Also, tasks in the following figure should be done under IT Management Process.

IT MANAGEMENT SYSTEM DESIGN

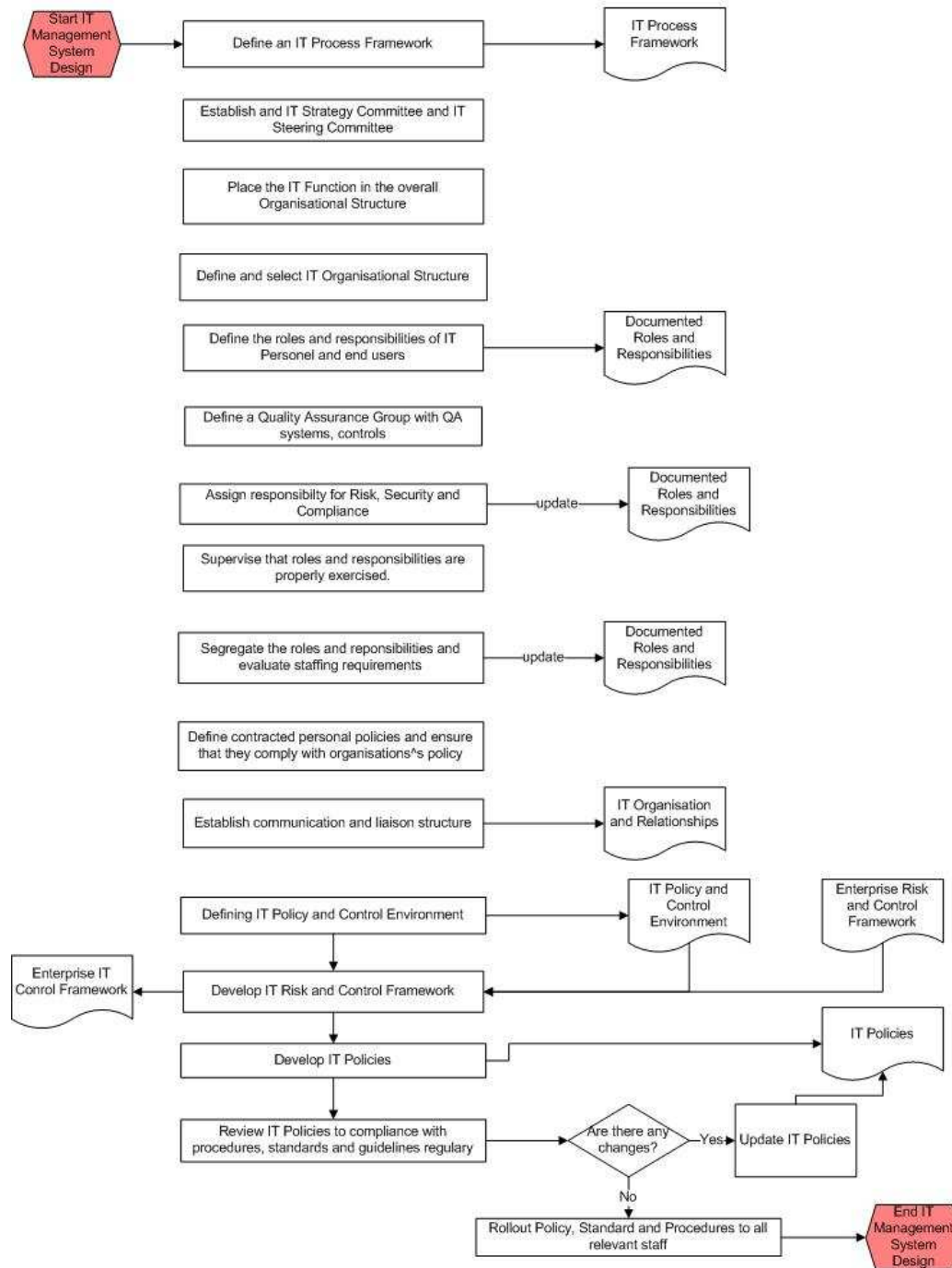


Figure 3-6 Tasks that should be done during IT management process

P.2 Portfolio Management

Principles:

1. There exist portfolio stages: established requirements, described, analyzed, approved, allocated resources and budget, design, development, build, test, deployed, operational and retired.
2. Contents of Service Portfolio: Service name, service definition, service status, service category and priority, used applications, data schema, supported business processes, business owner, business user, IT owner, warranty level, Service Level Agreements (SLA), Service Level Requirements (SLR), supporting services, supporting resources, dependent services, supporting Operating Level Agreements (OLA), contracts, service cost and service metrics.
3. The outcomes for existing services fall into six main categories;
 - a. Retain: services are relevant to organization's strategy
 - b. Replace: these services are unclear and overlapping business functionality
 - c. Rationalize: offering services that are composed of multiple releases of the same operating system, multiple version of same software.
 - d. Refactor: Refactoring core business services and reusable services
 - e. Renew: these services meet functional criteria but fail technical fitness
 - f. Retire: services that do not meet minimum levels of technical and functional requirements

General Information:

Table 3-4 General Information about Service Portfolio management process

Process ID	P.2
Process	Service Portfolio Management
Purpose	Portfolio management of IT based investments programmes to achieve strategic business objectives Maximizing value by keeping cost and risk at an acceptable level Reflecting business strategies and prioritization in portfolio
Scope	Taking planned works into portfolio by looking at resources Portfolio is categorized as three main parts : services in development stage, current services and retired services
Values to Business	Providing easy monitoring and controlling of IT by showing start and end date of procedures
Inputs	Updated Service Portfolio Updated Project Portfolio
Outputs	Service Portfolio Project Portfolio
Roles	IT Committee Product Manager Business Relationship Manager
Tools	Portfolio Management Tool
Metrics	Percent of deviation in works defined in portfolio Percent of updating portfolio

Flow Chart:

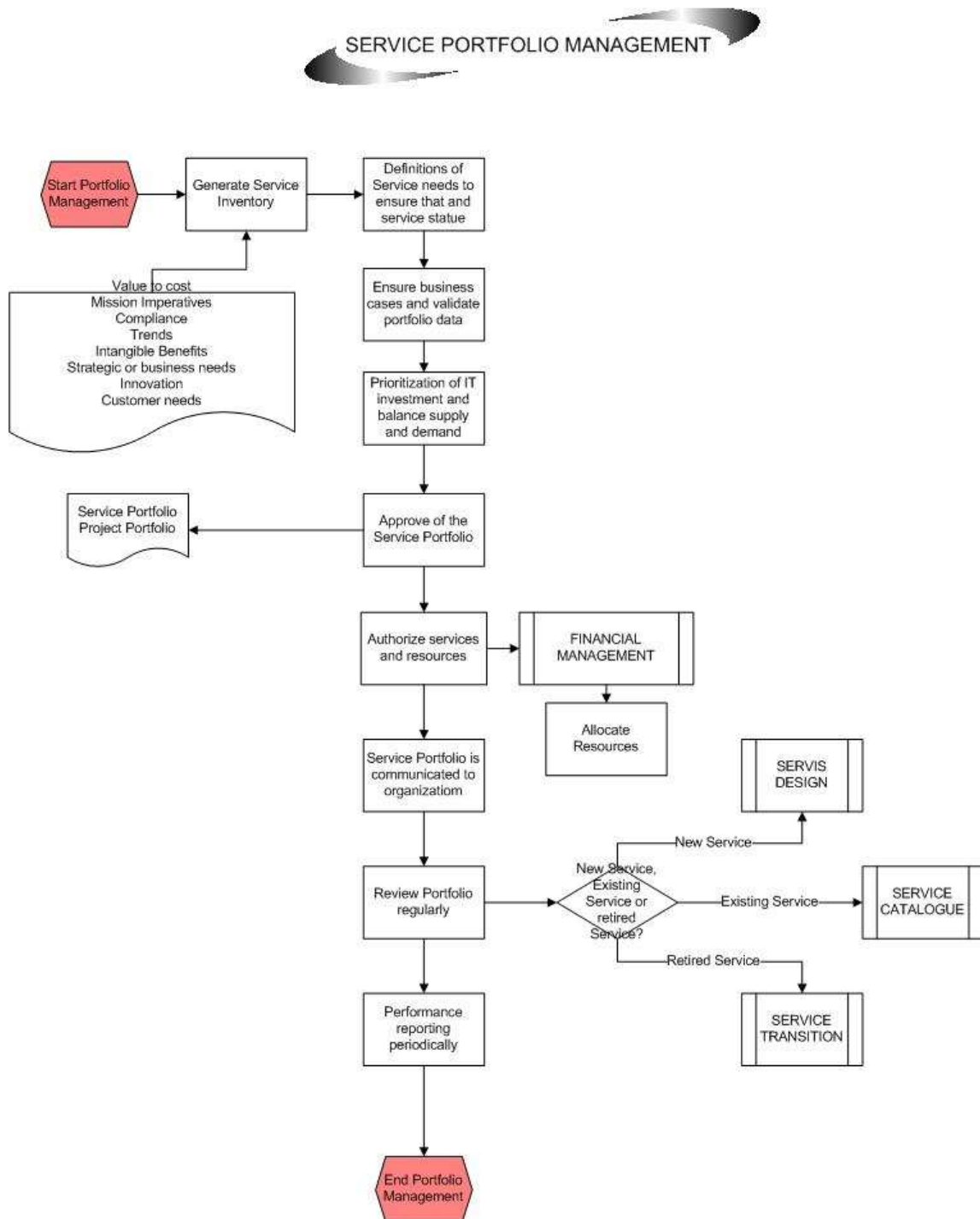


Figure 3-7 Flow chart of Service Portfolio management process

P.3 Financial Management

Principles:

1. Variable cost analysis is important issue. If it is not taken into consideration, there exist big deviations. Examples of variables that must be considered are;
 - a. Type and number of users
 - b. Number of software license
 - c. Types and number of resources
2. While evaluating IT costs, variable cost personnel and charge of employees are considered.
3. After evaluating IT costs, returning them to service costs are handled detail.
4. Financial effect of current service changes or future service demands should be evaluated and physical resources should be protected to keep on IT operation continuity.
5. Stages in financial management process are the following: Plan, Analysis, Design, Implement and Measure.
6. Charging of services increase the awareness of organization about IT costs.
7. While preparing budget, return on investment (ROI) and net present value (NPV) are evaluated. By using these values, accuracy of investment is decided. In addition to these values, abstract benefits are considered.
8. IT and business stakeholders provides usage of IT resources effectively and transparent of total cost of ownership.
9. The aim of establishing Financial Framework is that managing cost and investment of IT assets and services by handling IT budget, IT based investment and business case.
10. In addition to total IT budgeting, programme based individual budgeting has also prepared.

General Information:

Table 3-5 General Information about Financial management process

Process ID	P.3
Process	Financial Management
Purpose	<p>Defining methods for budgeting, cost calculation and service charging for service providers</p> <p>Providing IT cost, funding system prepared by business users and segregated IT usage and cost reporting system completely and accurately</p> <p>Alignment and tracing of IT budget with IT strategy and investment decision</p> <p>Making a decision about IT investment and portfolio decisions effectively</p>
Scope	<p>Making an estimation about budget and prepare budget</p> <p>Service investment analysis is done and define criteria</p> <p>Measure and evaluate business value against forecast</p> <p>Charging of delivered services according to quality and amount</p> <p>Financial value of services are calculated by adding service cost and service value contribution</p> <p>Prepare cost plan</p>
Values to Business	<p>Ensuring transparency and understanding of IT costs to users and business part</p> <p>Continuously and demonstrably improving IT's cost efficiency and its contribution to the business profitability.</p>
Inputs	<p>SLAs and OLAs</p> <p>Strategic and Tactical Plans</p> <p>Performance and capacity plan</p> <p>Infrastructure Requirements</p> <p>Project Plan</p> <p>Project and service portfolio</p>
Outputs	<p>Cost – Benefit Reports</p> <p>IT Budget</p> <p>Financial Information</p> <p>IT Cost Model</p>
Roles	Financial Manager
Tools	Interface with Configuration Management System (CMS) to manage cost for each CI and resource to generate data related to billing, reporting, chargeback and cost analysis.

Table 3-5 (Continued)

Process	Financial Management
KPI	Percent of projects with the benefit defined up front Percent of IT services whose IT costs are recorded Frequency of benefit reporting Percent of business users involved in the definition of cost models Percent of costs that are allocated automatically, manually.

Flow Chart:

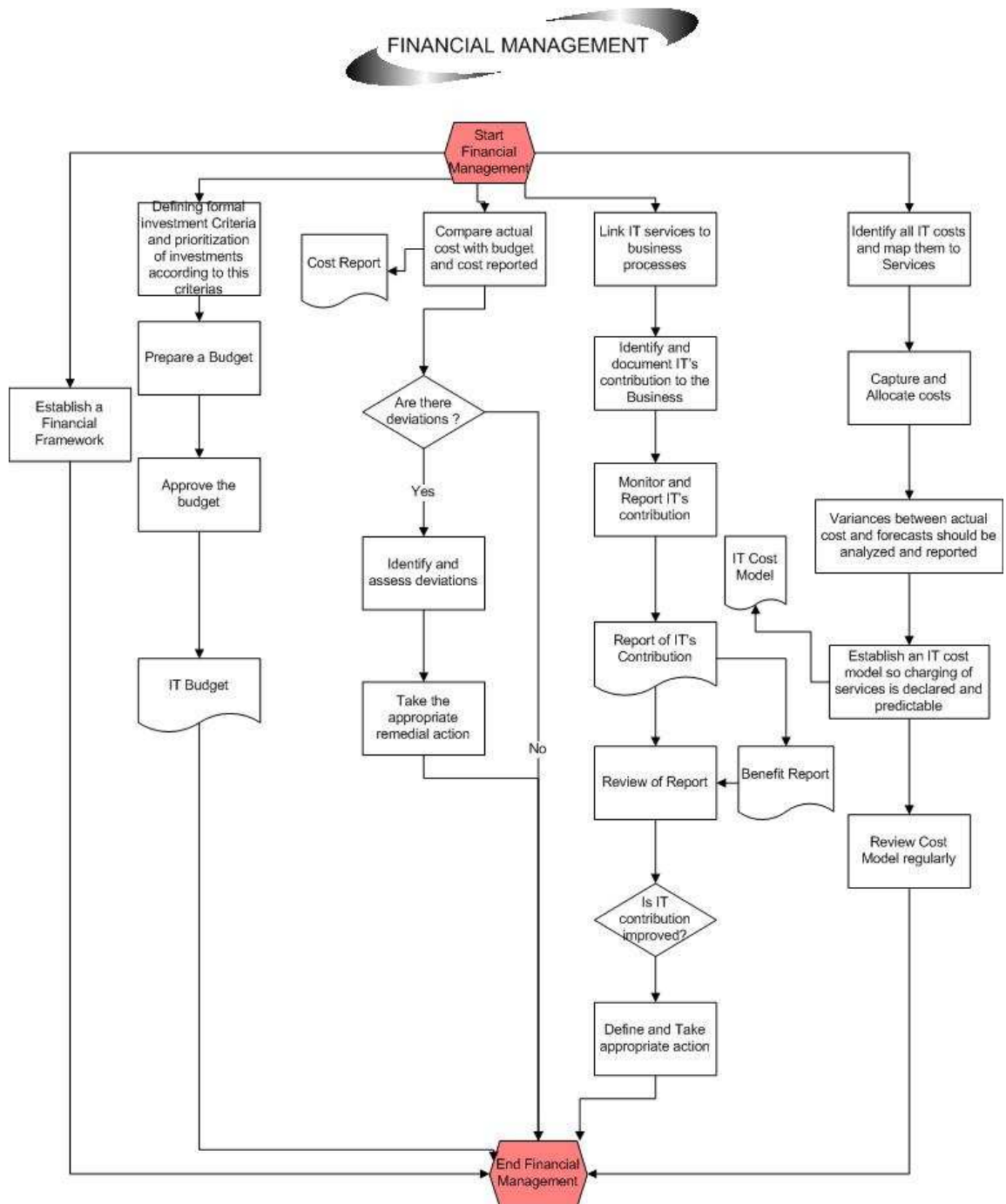


Figure 3-8 Flow chart of Financial management process

P.4 Corporate Architecture

Principles:

The definition of Corporate architecture according to Gartner is as the following; “the process of translating business vision and strategy into effective enterprise change, by creating, communicating and improving key principles and models that describe the enterprise’s future states and enable its evolution.”

Corporate Architecture process consists of service architecture, application architecture, IT infrastructure architecture and environment architecture.

IT Infrastructure architecture consists of the followings;

1. Applications and system software
2. Knowledge, data and data bases
3. Central server, mainframes, distributed local servers
4. Data networks
5. Client systems
6. Storage tools, storage domain networks, documents storage and management
7. Special areas of technology like EPOS, ATMs, scanners, GPS systems

General Information:

Table 3-6 General Information about Corporate Architecture process

Process ID	P.4
Process	Corporate Architecture
Purpose	Technology infrastructure plan for noticing technologic opportunities Defining and implementing architecture and standards
Scope	Establishing forum to direct technologic architecture Preparing technologic infrastructure plan balancing cost, risk and requirements Defining technologic infrastructure standards
Values to Business	Having stable, efficient in terms of cost and standard application systems, resources and capabilities to meet current and future business requirements

Table 3-6 (Continued)

Process	Corporate Architecture
Activities & Tasks	<p>Forming IT Architecture committee</p> <p>This committee is responsible for achieving design of IT architecture. In addition to this, the most important aim is to get clear and real expectation about what the technology delivers on account of product and service architecture guideline is prepared and make a recommendation of implementation of it.</p> <p>Assessing current and new technologies and choosing suitable technology direction to realize IT strategy and making plan</p> <p>Technologies creating potential business opportunities are defined in plan and this plan consists of infrastructure components system architecture, technologic direction and contingency directions</p> <p>IT technology plan should be suitable to IT strategic and tactical plan</p> <p>Technologic infrastructure plan is dependent to technologic direction and should consists of risk arrangements about acquisition of resources</p> <p>This plan also consists of changes that may occur in competitive environment</p> <p>Defining a method tracing and monitoring business sector, industry, technology, infrastructure, legal and regulatory environment trends</p> <p>Constituting and maintaining technology standards</p> <p>Providing technology instruction by constituting a forum which provides suggestion about the technology choice and so helps monitoring technology improvement</p>
Inputs	Strategic and Tactical Plans
Outputs	<p>Technology Infrastructure Plan</p> <p>Infrastructure Requirements</p> <p>Technology Opportunities</p> <p>Technology Standards</p>
Roles	<p>Corporate Architecture Responsible</p> <p>All personals</p>
Tools	Portal or Forum tools
KPI	<p>Frequency of meetings done by technology forum</p> <p>Frequency of meetings done by IT Architecture responsible</p> <p>Frequency of reviewing and updating of technology infrastructure plan</p> <p>Percent of inconsistency with defined technology standards</p>

Flow Chart:

There is not Flow chart for this process.

P.5 Risk Management

Principles:

1. Risk management framework contains acceptable level for risks, documenting residual risks and pull residual risks to an acceptable level by defining mitigation strategies
2. Risks are recorded and maintained.
3. Probability of occurring risks is assessed by quantitative and qualitative methods.
4. Risk Mitigation Methods;
 - Getting addition UPS
 - Set up a Fault tolerant systems
 - Holding alternative supplies
 - Comprehensive backup system
5. Risk strategies are defined as the following;
 - Avoidance
 - Reduction
 - Sharing
 - Acceptance
6. Cost, benefit and responsible of risk remediation plans are defined.
7. After implementing risk remediation plans, any variance is reported to executive manager.

General Information:

Table 3-7 General Information about Risk management process

Process ID	P.5
Process	Risk Management
Sub Process	There exist two phase: Risk Analyze and Risk Management
Purpose	Risks are evaluated and potential benefits are analyzed. For each action, risks and opportunities are defined and suitable reactions are identified.
Scope	Ensuring that risk management is integrated into management process and risk management is implemented continuously and consistently Making risk evaluation Proposing and delivering risk remediation plans
Values to Business	Analyzing and announcing IT potential risks effect into the business processes and goals
Inputs	Security threads and gaps Supplier risks Project risk management plan IT strategic and tactical plans History risk trends Contingency Test Results
Outputs	Risk Assessment Risk Reporting IT Risk Management Guideline IT Risk Remediation Plan
Roles	Risk Manager
Metrics	Percent of IT conditions assessed Percent of IT risks defined newly Number of incidents results from risk defined in risk management process Percent of critic IT risks developed remediation plans against

Flow Chart:

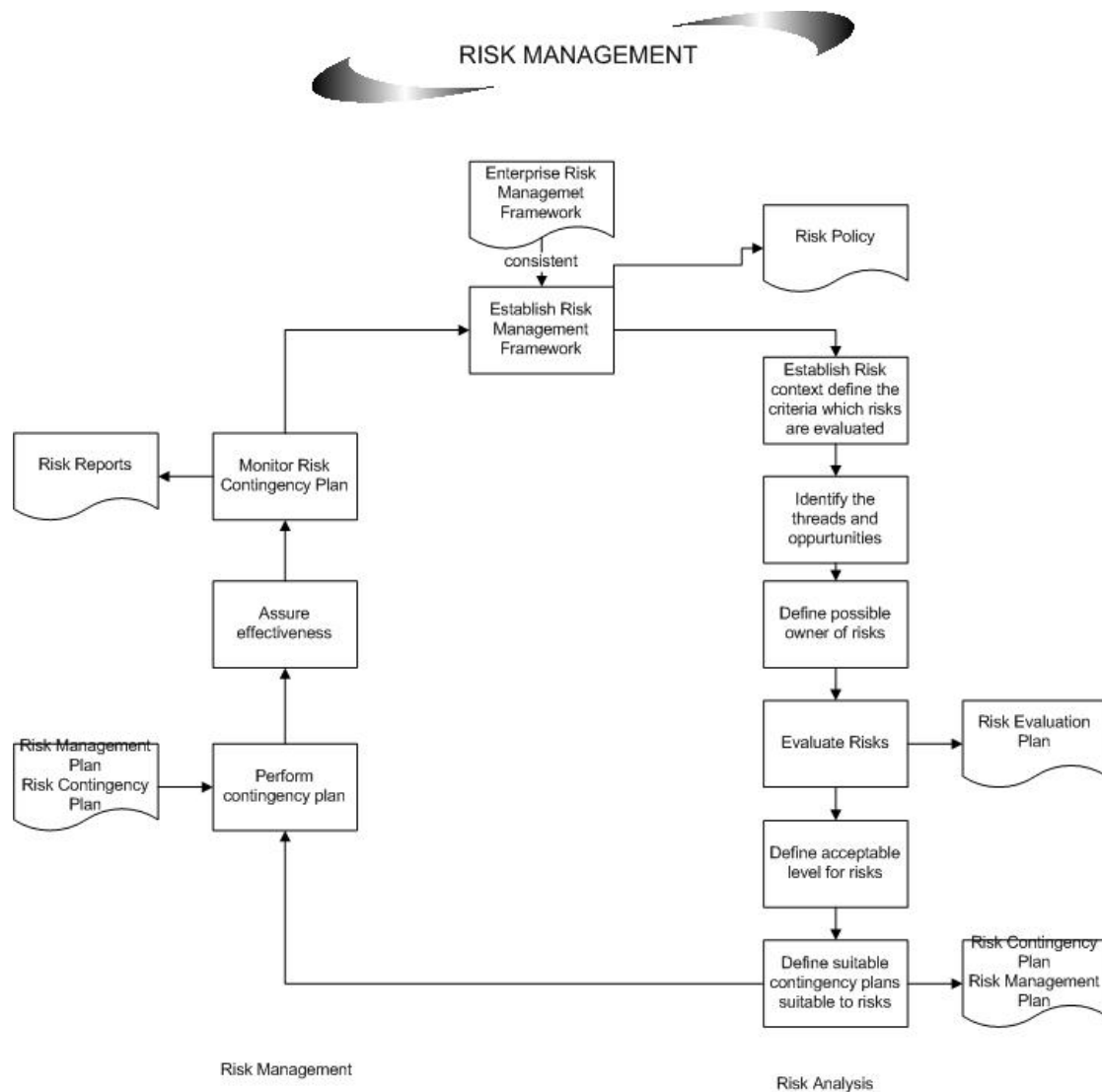


Figure 3-9 Flow chart of Risk management process

P.6 Software Development Lifecycle Management

Principles:

1. Three types of requirements exist: Functional, Non-Functional and Usability requirements.
2. Functional requirements are task of services. While showing task of services, one of the context diagram, use case, data flow or object diagram can be used.

3. Non-functional requirements define constraints and needs on service.
4. Categories of non-functional requirements: manageability, efficiency, availability and reliability, capacity and performance, security, installation, continuity, controllability, maintainability, operability, measurability and reportability.
5. Gathering requirements methods:
 - a. Negotiations
 - b. Workshops
 - c. Observation
 - d. Protocol analysis
 - e. Shadowing
 - f. Scenario analysis
 - g. Prototyping
6. Requirements should be SMART. (Specific, measurable, achievable, realistic and timely)
7. Each requirement should have an ID, resource, owner and priority.
8. Some software can be used to manage changes on documents like CARE, CASE.
9. Application security and availability requirements are identified. These requirements are realized against risks defined by taking account of data classification, information architecture, and information security.
10. If there are any changes on existing application, all steps defined in software lifecycle are carried out.
11. While developing application software, quality assurance requirements and approval standards are used which are defined in Quality management like design documents, development and documentation standards.
12. Software quality assurance plan is prepared to provide consistency with quality defined in requirements document.
13. Individual requirements' statue is tracked and if it needs any change, then Change management processes is activated.

General Information:**Table 3-8 General Information about Software Development Lifecycle process**

Process ID	P.6
Process	Software Development Lifecycle
Purpose	Developing software suitable to business requirements. Developing process timely and cost effective.
Scope	Transform business requirements into design Dependent on development standards for all modifications Separate development, test and operational activities
Values to Business	Aligning existing application with business requirements timely and cost effective
Activities & Tasks	Business Requirements Software Requirements High level design Detailed Design Coding
Inputs	Business requirements feasibility study Development Standards Cost – benefit reports Project Plan Data dictionary Data classification schema
Outputs	Scripts used before and after deployment Scripts which are necessary to start and stop application Scripts necessary for controlling software and hardware configurations before and after deployment Metrics for evaluating application performance SLA / OLA objectives and requirements Documents Application restore and back up Application security control conditions
Roles	Developer Software Manager Software Configuration Manager
Tools	Requirements management tool Design tools Software test tools Software configuration tool

Table 3-8 (Continued)

Process	Software Development Lifecycle
KPI	Percent of projects developed on time and on budget Percent of effort spend for maintaining existing applications Number of production problems per applications causing downtime Reported defects per function point per month

Flow Chart:

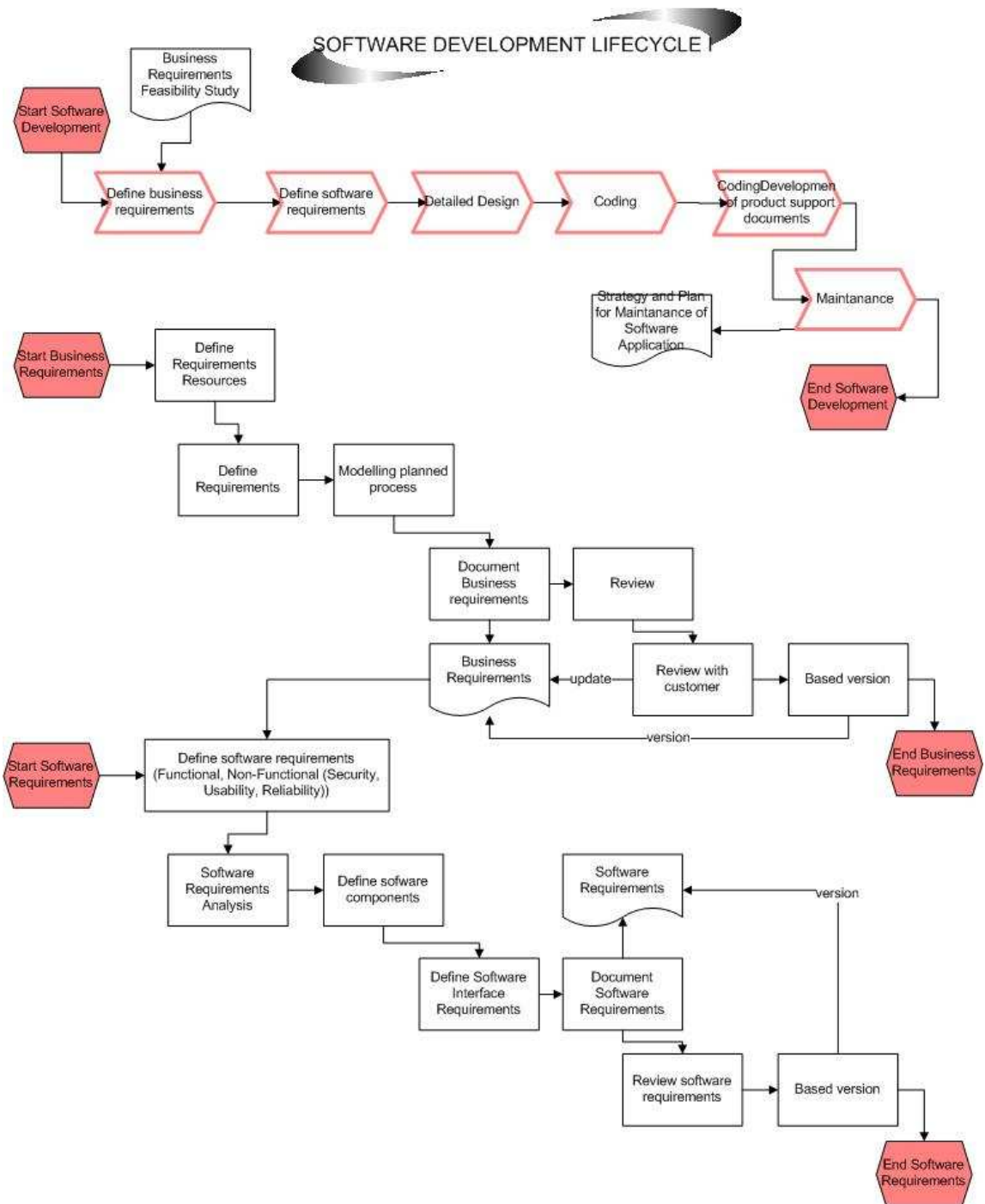


Figure 3-10 Flow chart of Software Development Life cycle process

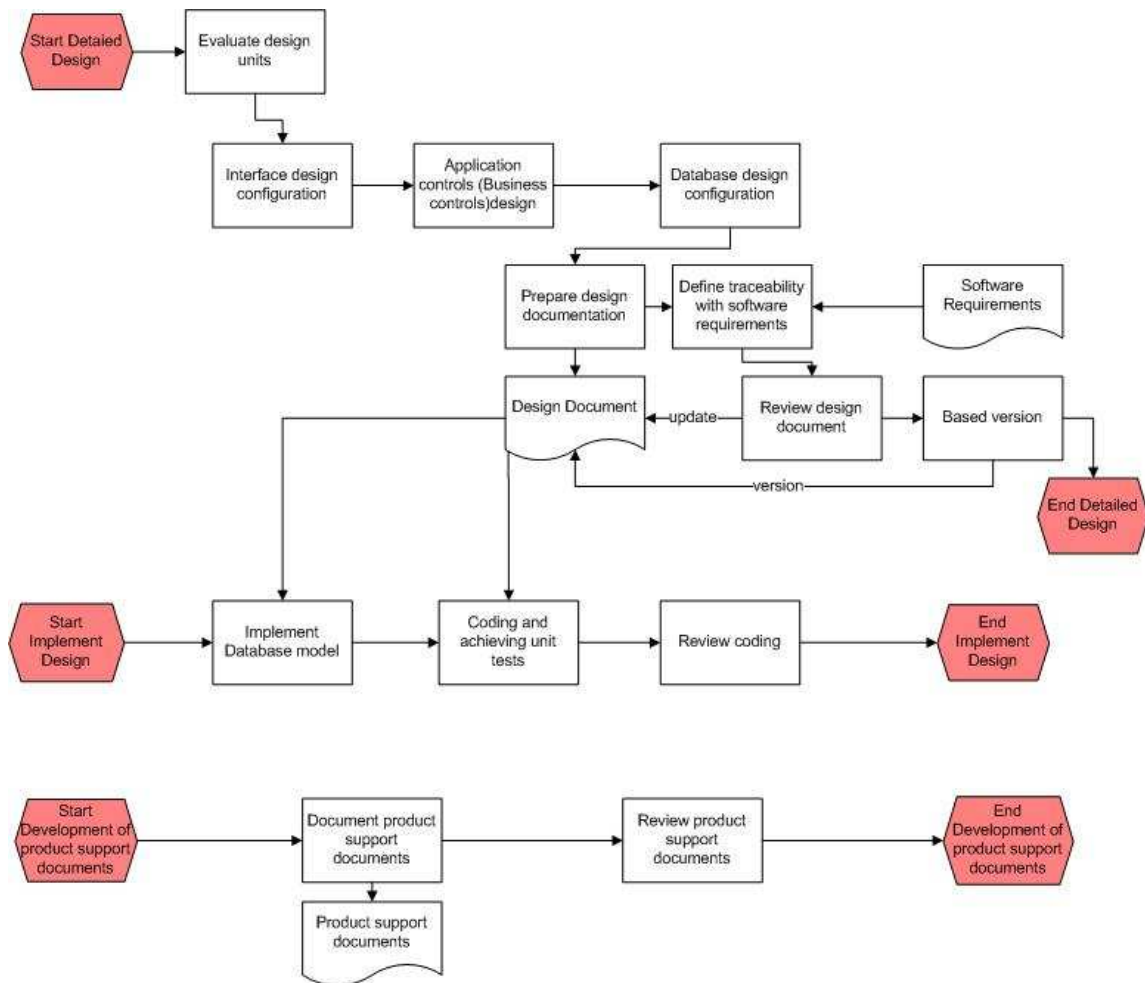


Figure: 3-10 (Continued)

P.7 Service Catalogue Management

Principles:

1. Organizations decide and define what services are.
2. The level of details of services is decided and statue of services is appointed.
3. Policy about the Service Catalogue is published.
4. Not only business services, supporting services should also be in Service Catalogue.
5. All services are categorized as technical or business.

6. Any changes to service catalogue or service portfolio is handled by Change Management Process.
7. Organization should define both business and technical catalogue. The recommended method is that defining a one catalogue contains both of them.
8. Information in service catalogue should be consistent with Service Knowledge Management System (SKMS) and CMS.
9. Information is aligned to the business and business processes by interfacing with Business relationship management.
10. Service Catalogue example is given in Appendix E.

General Information:

Table 3-9 General Information about Service Catalogue management process

Process ID	P.7
Process	Service Catalogue Management (SCM)
Purpose	The purpose of SCM is to manage the information in Service Catalogue and to ensure that it is accurate and reflect the current details, status, interfaces and dependencies of all services that are being run or being prepared to run in the live environment.
Scope	Providing and protecting consistent and standard information source about all agreed services Definition of service Production and maintaining of accurate Service Catalogue Providing a relationship between service catalogue and service portfolio Dependencies between all services and supporting services and dependencies between supporting components and Configuration Items (CI) in Service catalogue and CMS.
Values to Business	All areas of business can view an accurate, consistent picture of the IT services, their details and their status.
Inputs	Business impact analysis (impact, priority and risk associated with each service or changes to service requirements) Supplier Services CMS Service portfolio Feedback from all other processes Updated Service Catalogue

Table 3-9 (Continued)

Process	Service Catalogue Management (SCM)
Outputs	Definition of service Updated service portfolio Service catalogue
Roles	Service Catalogue Manager
Tools	CMS / SKMS
KPI	<p>Number of services recorded and managed in Service catalogue as a percentage of those being delivered and transitioned into live environment</p> <p>The number of variances detected between the information contained in service catalogue and 'real world' situation</p> <p>Business' users awareness of the services being provided</p> <p>Percentage increase in completeness of the Business Service Catalogue against operational services.</p> <p>IT staff awareness of technology supporting the services</p> <p>Service desk having access to information to support all live services measured by the percentage of incidents without the appropriate service related information.</p> <p>Percentage increase in completeness of the Technical Service Catalogue against the IT components.</p>

Flow Chart:

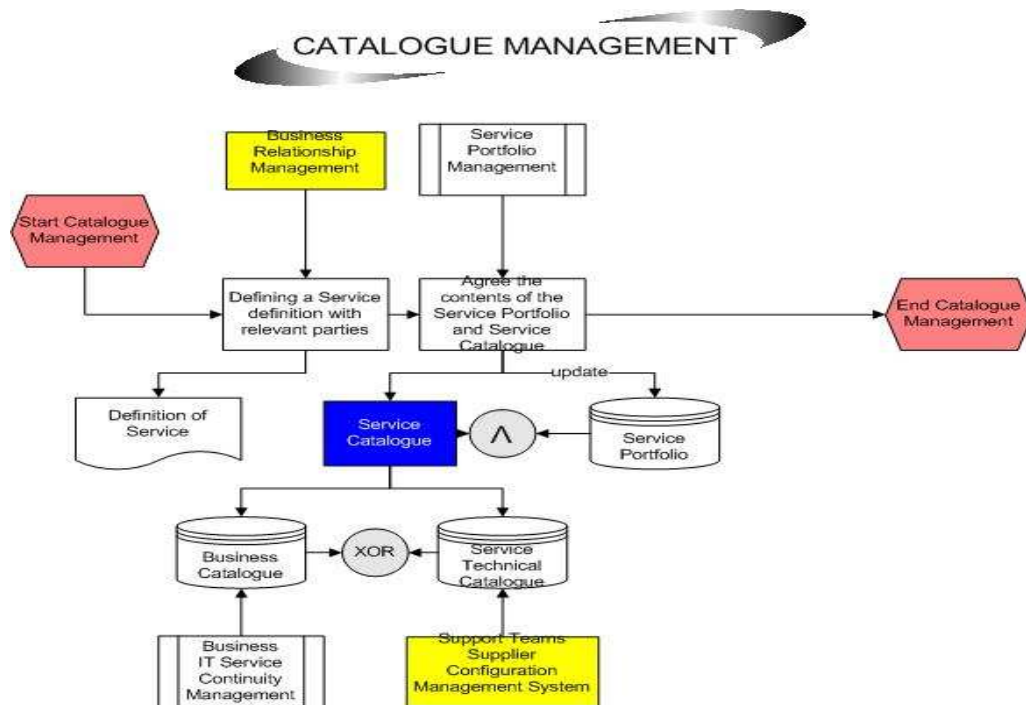


Figure 3-11 Flow chart of Service Catalogue management process

P.8 Service Level Management

Principles:

1. Service Level management is related to new gathered requirements for existing services and it provides improvement of SLA of services to meet business requirements and expectations.
2. While preparing SLA, It should not be designed according to only one part. Right balance and relation between IT service provider and customer provides beneficial agreement. All targets defined in SLA should be supported by underpinning contracts, OLAs and agreements with business. All measurements should be evaluated.
3. SLA is a agreement which contains both service provider and customer responsibilities and objectives.
4. SLA is used for measuring whether services meets customer needs or not.
5. In addition to this, SLA strengthens the communication between IT and customer.
6. SLA is used by most of processes defined like Problem Management, Incident Management, Change Management, etc.
7. SLA is divided into three parts: Service based, customer based and multilevel.
8. SLAs should be traceable and measurable.
9. OLA is agreement made between IT service provider and supplier exists in the same organization. OLAs can support more than one SLA.
10. Underpinning contracts are agreement made by IT service provider and suppliers.
11. Service reports should not only contain current performance, it should also contain previous performance.
12. Service Manager defines and implements actions necessary to renew service quality and overcome difficulties with Quality Manager. And both of them activate Service Improvement Plan (SIP) explained detail in Quality Management.

13. SLA and OLA example is given in Appendix C.

General Information:

Table 3-10 General Information about Service Level management process

Process ID	P.8
Process	Service Level Management (SLM)
Purpose	<p>Aligning key IT services and business strategy</p> <p>Manage IT services level</p> <p>Manage business and customer relationship</p> <p>Ensure that proactive metrics are implemented to improve services level</p> <p>Make certain that all operational services and their performance are measured professionally and coherent through all organization and services and produced reports meet business and customer needs</p> <p>SLM negotiate, decide and document IT service objectives with business representative and after that monitor these objectives and produce reports to deliver decided service level in the capability of service provider.</p>
Scope	<p>Provide a communication to the business and customers</p> <p>SLM manages the expectation and perception of the business, customers and users expectation and perception</p> <p>Ensure that the quality of service is matched to those expectations and needs.</p> <p>SLM provides SLAs, SLRs and OLAs.</p> <p>Review of suppliers agreements</p> <p>Review of SLAs</p> <p>Prevent service failures proactively, Mitigate service risks and improve service quality</p> <p>Manage and report all services and review SLAs breaches and weakness</p>
Values to Business	SLM provides reliable communication channel and trusted relation between customer and business representatives

Table 3-10 (Continued)

Process	Service Level Management (SLM)
Inputs	Service Catalogue Service Portfolio Business Information Business Impact Analysis Incident response times, impact definitions Business Requirements Changes to services CMS Customer and User Feedback Initial planned SLA and OLA
Outputs	Service Performance Reports SIP Service Quality Plan SDP SLAs SLRs OLAs Service Review Meetings SLA review and Service scope review Revised SLAs, contract, OLAs Service Information Service Management Plan
Roles	Service Level Manager
KPI	Percentage reduction in SLA targets missed Percentage reduction in SLA targets threatened Percentage increase in customer perception and satisfaction of SLA achievements Percentage reduction in SLA breaches caused because of third party support contracts Percentage reduction in SLA breaches caused because of OLAs Percentage and number of services covered by SLA Percentage reduction in cost of monitoring and reporting SLA Percentage increase in improving suitable SLA Frequency of service review meetings

Flow Chart;

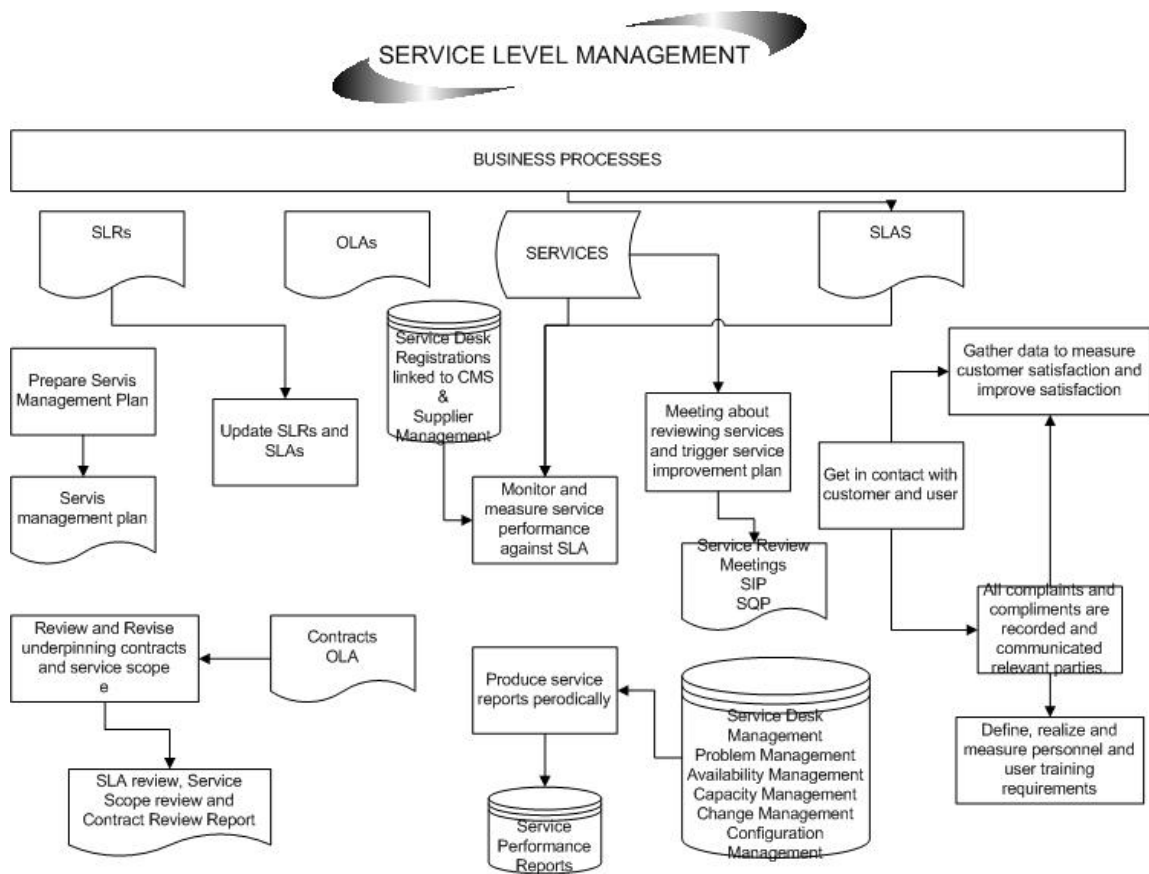


Figure 3-12 Flow chart of Service Level management process

P.9 Configuration Management

Principles:

1. Develop and maintain service asset and configuration policies
2. Defining configuration models (contains configuration items and their relationship)
3. Generate Configuration Management Data Base (CMDB) (contains information about personnel, supplier, location, business units, information about customer and users)

4. Defining Configuration Management System (CMS) (CMDB, secure library and secure stores, The definitive Media Library, Definitive Spares, Configuration baseline and snapshot)
5. Attributes of Configuration Items kept on database are the following;
 - a. Unique Identifier
 - b. CI type
 - c. Name/description
 - d. Version
 - e. Location
 - f. Supply Date
 - g. License details
 - h. Owner
 - i. Status
 - j. Related document masters
 - k. Related software masters
 - l. Relationship type
 - m. Applicable SLA

General Information:

Table 3-11 General Information about Configuration management process

Process ID	P.9
Process	Configuration Management
Purpose	Identify control, record, report, audit and verify service assets and CIs. Account for and management of integrity of service assets Ensure integrity of CIs by establishing and maintaining CMS.
Scope	Components of a complete service, system or product are identified and maintained and changes to them are controlled. Ensures that any changes done on CMS is done by approvals. All configuration items are defined and maintained. Integrity of configurations data is reviewed.
Values to Business	Optimizing the performance of service assets and configurations improves the overall service performance and optimizes the cost and risk caused by poorly managed assets.
Inputs	Released Configuration Items New, changed or disposed assets or configuration items Criticality of CI
Outputs	RFC Configuration Management System (CMS) Configuration Management Plan
Roles	Service Asset and Configuration Manager Configuration Administrator
Tools	Configuration Management System software consist of details about the each CI s and their relationships. Discovery and audit tools Relation between configuration items and services
KPI	Percentage improvements in maintenance scheduling over the life of an asset Degree of alignment between provided maintenance and business support Assets identified as the cause of incidents Improved speed for incident management to identify faulty CIs and restore services Impact of incidents and errors affecting particular CI types Ratio of used licenses against paid for licenses Percentage reduction in business impact of outages and incidents caused by poor asset and configuration management

Flow Chart:

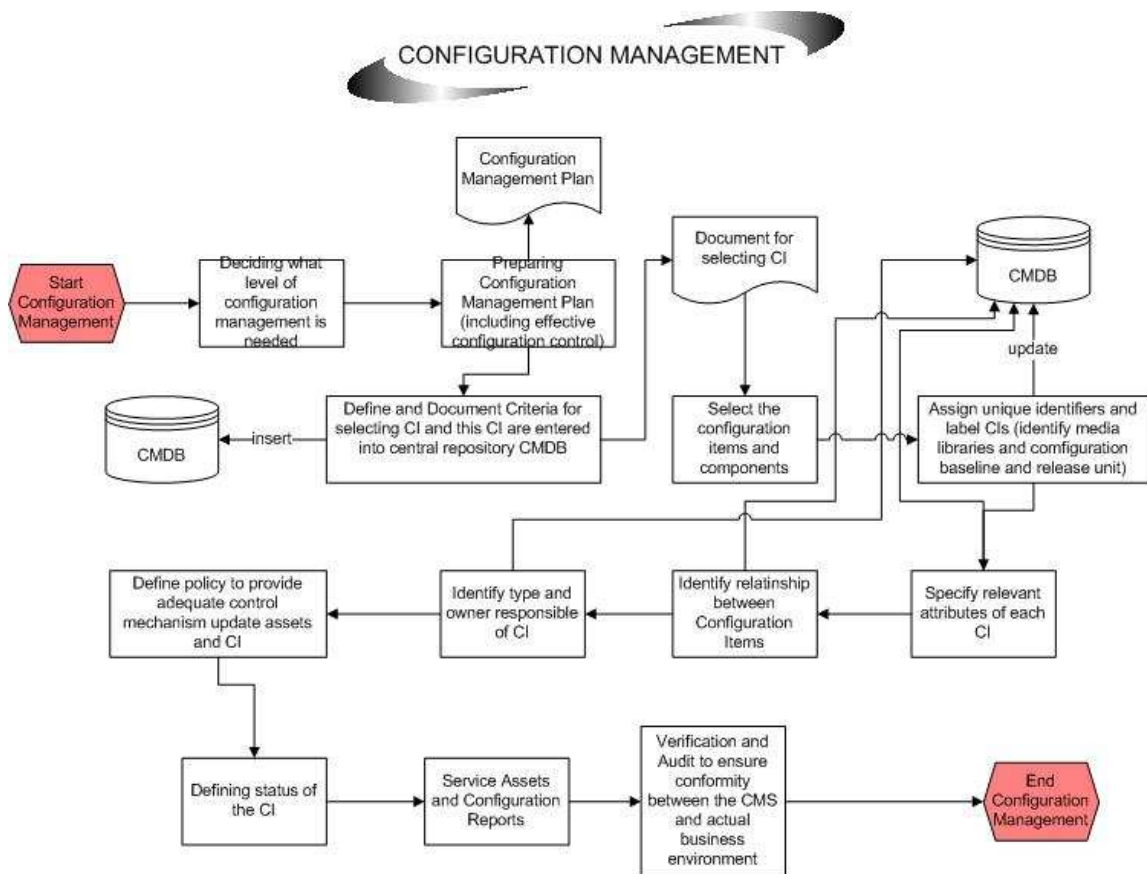


Figure 3-13 Flow chart of Configuration management process

P.10 Capacity management

Principles:

1. Capacity management is both proactive and reactive. The more proactive it needs less reactive management.
2. Capacity management balance cost against resource needs.
3. It balances demand against supply.
4. Capacity management aligns IT resources and capacity with continually changing business requirements and needs with effective and efficient cost.
5. Plan should be generated containing current resource usage and service performance. Future requirements are estimated and documented by taking into

consideration of service strategy and plan in capacity plan. Financial data is important for estimating future capacity requirements.

6. Capacity management should be directly related to service strategy and portfolio.
7. This process provides efficient information to all other service management processes. (whether capacity is enough for SLA or not, whether problem is aroused from capacity or not)
8. Capacity management contains three sub processes which are business capacity management, service capacity management and component capacity management.
9. Business capacity management (Translates business needs and plans into requirements for service and IT infrastructure, ensuring that future business requirements for IT services are quantified, designed, planned and implemented in a timely fashion.)
 - ✓ Business capacity management helps deciding service level requirements.
 - ✓ It should be included in the design of new or changed services and propose hardware and software procurement.
 - ✓ Supporting SLA reviews and verify SLA
10. Service capacity management (Manage, control and estimate performance and capacity of live, operational IT services from end to end)
 - ✓ Defining and understanding resource usage and patterns of operation of IT services and ensure that these services meet SLA objectives.
11. Component capacity management (Manage, control and estimate performance, usage and capacity of IT technology components)
 - ✓ Define and understand each component's performance, capacity and usage
 - ✓ Components are infrastructure, environment, data and applications. All these components should be monitored and controlled.
12. While analyzing and fixing issues about capacity, some methods can be used;
 - ✓ Deciding intensive times when services are used mostly, then some arrangements can be done about service usage at intensive times
 - ✓ Improvements about those services can be defined.

13. Identifying future capacity requirements by making trend analyzing, modeling (analytic modeling, simulation) and baselining.
14. An example of a capacity plan is given in Appendix G.

General Information:

Table 3-12 General Information about Capacity management process

Process ID	P.10
Process	Capacity Management
Purpose	Capacity management focuses on performance and capacity related issues, relating to both services and resources.
Scope	<p>The process should encompass all areas of technology, both hardware and software for all IT technology components. Should also consider space planning and environmental capacity as well as human resources.</p> <p>The scheduling of human resources, staffing levels, skill levels and capability levels should be included.</p> <p>New technology needs to be understood and used to innovate and deliver the services.</p> <p>Capacity plan reflecting current and future business requirements is generated and reviewed.</p> <p>It is suggested and directed to all business and IT areas about all capacity and performance issues.</p> <p>IT supports solution of incidents and problems about performance and capacity.</p> <p>Evaluate effect of changes on service and resources' capacity and performance.</p> <p>Capacity management improves service performance proactively and sustainable cost.</p>
Values to Business	Capacity management provides IT resources to be planned and scheduled to provide a consistent level of service that is matched to the current and future needs of the business as agreed and documented within SLAs and OLAs.
Activities & Tasks	<p>Assists with agreeing Service Level Requirements</p> <p>Design, procure or amend service configuration</p> <p>Verify SLA</p> <p>Support SLA Negotiation</p> <p>Control and Implementation</p>

Table 3-12 (Continued)

Process	Capacity Management
Inputs	Service Capacity Plan Service Performance Information Service Information Financial Information Change Information CMS Workload Information
Outputs	Capacity Management Information System The Capacity Plan Service Performance Information and reports Workload analysis and reports Threshold, alerts and events
Roles	Capacity Manager
KPI	Production of workload forecasts on time Percentage accuracy of forecasts of business trends Timely incorporation of business plans in to the capacity plan Reduction in the number of variances from the business plans and capacity plans Increased ability to monitor performance and throughput of all services and components Timely justification and implementation of new technology in line with business requirements Reduction in the use of old technology, causing breached SLAs due to problems with support or performance Reduction in last-minute buying to address urgent performance issues. Reduction in the superfluous capacity usage of IT Accurate forecast of planned expenditure Reduction in the interruption because of insufficient IT capacity Reduction in the cost of developing capacity plan Reduction in the number of incidents because of poor performance Reduction in the losses of business because of insufficient capacity Increase in advices done by capacity management Reduction in the SLA breaches because of weak service performance or component performance

Flow Chart:

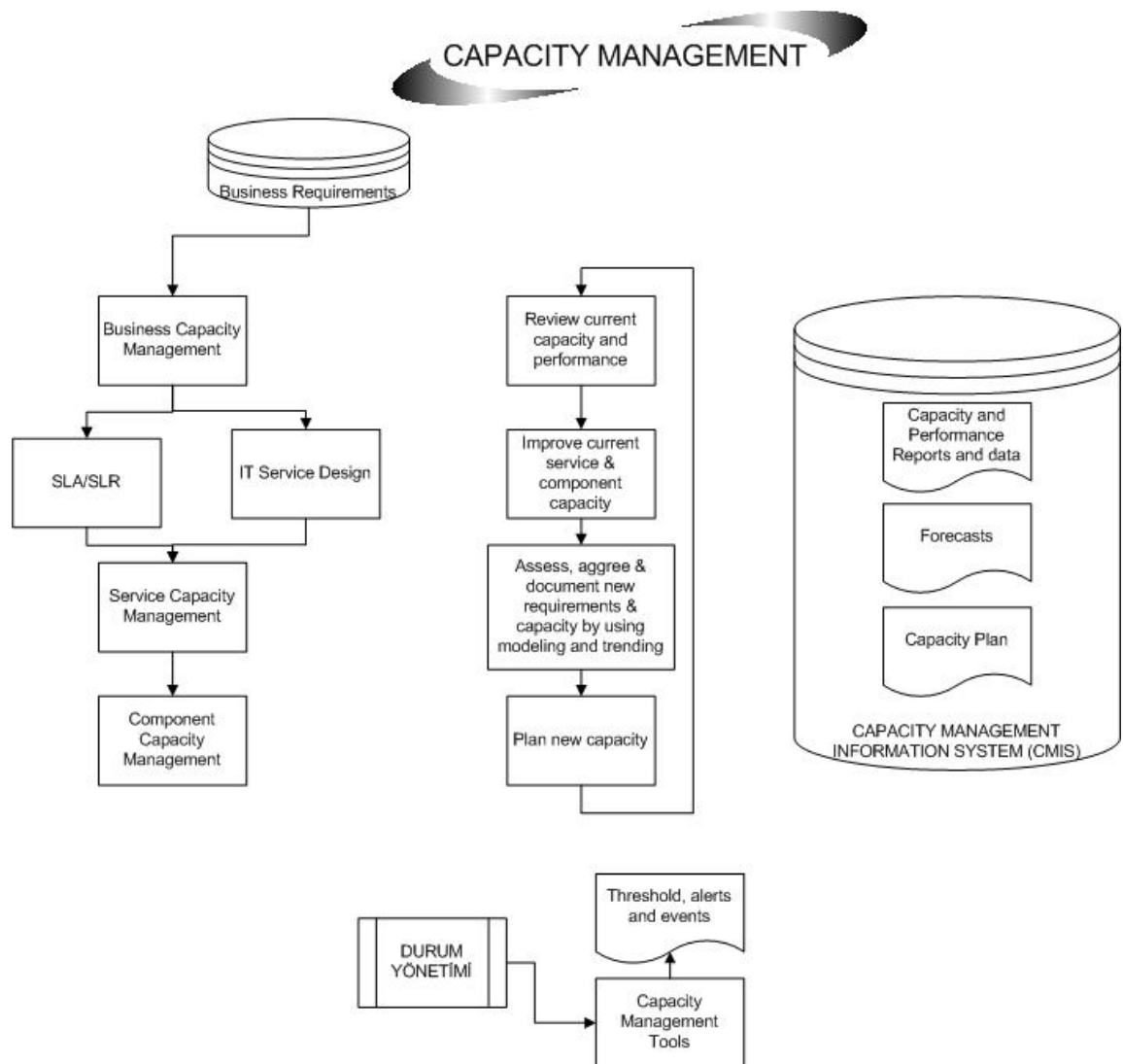


Figure 3-14 Flow chart of Capacity management process

P.11 Continuity Management

Principles:

1. Continuity management is a cyclic process that once a continuity and salvage plan is prepared then always these documents should be updated according to “business continuity plan” and “business priorities”.

2. The definition of Business Impact Analysis (BIA) is to define effect of service loss on business.
3. Recovery Options;
 - ✓ Manual work-around
 - ✓ Reciprocal arrangements
 - ✓ Gradual recovery
 - ✓ Intermediate recovery
 - ✓ Fast recovery
 - ✓ Immediate recovery
4. Test types;
 - ✓ Walk-through tests
 - ✓ Full tests
 - ✓ Partial tests
 - ✓ Scenario tests
5. Addition to the Continuity plan, Emergency Response Plan, Damage Assessment Plan, Salvage Plan, Vital Records Plan, Crisis Management and Public Relations Plan, Accommodation and Services Plan, Security Plan, Personal Plan, Communication Plan and Finance and Administration Plan can be added.
6. Off Site backup should be defined.
7. The content of IT continuity plan is as the following;
 1. Management
 - a. When and how the plan is activated
 - b. Details of IT infrastructure (hardware, software), contracts and agreements supporting recovery
 2. IT Infrastructure
 - a. IT components covered during continuity management
 3. Operational Procedures
 - a. Steps needed for restarting operations, SLA details and manuals
 4. Personnel

- a. Personnel and alternative of them charged in emergency cases
- 5. Security
- 6. Contingency site
 - a. Location, personnel made contract, prepared infrastructure, etc.
- 7. Recovery
 - When, where and how much time?

General Information:

Table 3-13 General Information about IT Service Continuity management process

Process ID	P.11
Process	IT Service Continuity Management (ITSCM)
Purpose	Maintaining the necessary ongoing recovery capability with in IT services and their supporting components.
Scope	ITSCM focuses on disaster events determined significantly by business
Values to Business	Recovery arrangements of IT services are aligned to identified business impacts, risks and needs and ITSCM implement Business Continuity Plan.
Inputs	A Business Continuity Strategy and Plan Service Information Change Information CMS Business Continuity Management testing Schedules IT Service Continuity Plans from Suppliers and partners Risk assessment / Risk remediation plan SLA and OLA
Outputs	ITSCM policy and strategy Business Impact Analysis A set of ITSCM plans ITSCM testing schedules ITSCM test scenarios ITSCM test reports Contingency test results IT Service Continuity Plan Critical IT CIs Backup storage and protection plan
Roles	IT Service Continuity Manager

Process	IT Service Continuity Management (ITSCM)
KPI	Review continuity plan continuously All service recovery targets are defined in SLAs and gathered from continuity plans Manage continuity contracts with third parties Awareness of business effect, needs and requirements

```

graph TD
    Start([Start ITSCM]) --> Scope[Determine the scope of the ITSCM process and the policies]
    Scope --> Rules[Create rules and structures to document, test and execute the disaster recovery and IT contingency Plans]
    Rules --> Org[Define the organizational structure for continuity management (roles, responsibilities, tasks,...)]
    Org --> Project[Define the project organization and control structure]
    Project --> Resources[Allocate Resources]
    Resources --> BIA2[Business Impact Analysis]
    BIA2 --> DefineCIR[Define Critical IT Resources]
    DefineCIR --> Overall[Produce an overall ITSCM strategy integrated with BCM strategy]
    Overall --> DefineOptions[Define ITSCM recovery Options]
    DefineOptions --> RiskPlans[Risk Remedial Action Plans]
    RiskPlans --> DefineOptions
    DefineOptions --> ICP1[IT Continuity Plan]
    ICP1 --> BusinessPlan[Business Continuity Plan]
    BusinessPlan --> ICP1
    ICP1 --> TestPlan[Test the IT Continuity Plan]
    TestPlan --> BIA1[Business Impact Analysis]
    BIA1 --> DefineCIR
    DefineCIR --> BIA1
    DefineCIR --> BIAEx[BIA exercises and reports]
    BIAEx --> TestPlan
    TestPlan --> ICP2[IT Continuity Plan]
    ICP2 --> Supplier[Supplier Continuity Management Plan]
    Supplier --> ICP2
    ICP2 --> Training[IT Continuity Plan Training]
    Training --> Maintenance[Maintainance of the IT Continuity Plan]
    Maintenance --> Info[Change Information]
    Info --> Maintenance
    Maintenance --> Changes{Are there any changes ?}
    Changes -- Yes --> ChangeMgmt[CHANGE MANAGEMENT]
    ChangeMgmt --> DefineOptions
    Changes -- NO --> Distribute[Distribute the IT Continuity Plan]
    Distribute --> Review[Post-resumption Review (Prepare prosedure to evaluate ITSCM plan efficiency after disaster and evaluate and update plan according to this prosedure)]
    Review --> End([End ITSCM])
  
```

The flowchart illustrates the IT Service Continuity Management (ITSCM) process. It begins with 'Start ITSCM', leading to 'Determine the scope of the ITSCM process and the policies', 'Create rules and structures to document, test and execute the disaster recovery and IT contingency Plans', and 'Define the organizational structure for continuity management (roles, responsibilities, tasks,...)'. This leads to 'Define the project organization and control structure', 'Allocate Resources', and 'Business Impact Analysis'. 'Business Impact Analysis' leads to 'Define Critical IT Resources', which then leads to 'Produce an overall ITSCM strategy integrated with BCM strategy'. This strategy leads to 'Define ITSCM recovery Options', which leads to 'Risk Remedial Action Plans' and 'IT Continuity Plan'. 'IT Continuity Plan' leads to 'Business Continuity Plan', which leads to 'IT Continuity Plan'. 'IT Continuity Plan' leads to 'Test the IT Continuity Plan', which leads to 'Business Impact Analysis', 'BIA exercises and reports', and 'IT Continuity Plan'. 'Test the IT Continuity Plan' leads to 'IT Continuity Plan Training', which leads to 'Maintainance of the IT Continuity Plan'. 'Maintainance of the IT Continuity Plan' leads to 'Change Information', which leads to 'Maintainance of the IT Continuity Plan'. 'Maintainance of the IT Continuity Plan' leads to a decision 'Are there any changes ?'. If 'Yes', it leads to 'CHANGE MANAGEMENT', which leads to 'Define ITSCM recovery Options'. If 'NO', it leads to 'Distribute the IT Continuity Plan', which leads to 'Post-resumption Review (Prepare prosedure to evaluate ITSCM plan efficiency after disaster and evaluate and update plan according to this prosedure)', which leads to 'End ITSCM'.

66

P.12 Availability Management

Principles:

1. Availability management has a close relationship with Risk management and Continuity management in terms of risk assessment and risk mitigations.
2. When services or components are unavailable, it helps to define and solve incidents or problems. Because of this reason, availability management works close with incident and problem management.
3. Service availability is very important for customer satisfaction and business success. Although service is unavailable, making service running as soon as possible increases the satisfaction of customer and user.
4. Availability can be improved by understanding that how IT services support business operations.
5. Service availability is important as much as weakest round of chain.
6. Availability is not only reactive, it is also proactive process.
7. Availability objectives are determined by business as Vital Business Function (VBF) not by IT.
8. The definition of VBF is that it is showed the critical business functions supported by IT services.
9. Some calculations can be made to evaluate availability of services;

Availability is composed of availability, reliability, maintainability and serviceability.

Availability: the ability of a service, component or CI to perform its agreed function when required. It is measured by;

$$\text{Availability \%} = \frac{\text{Agreed Service Time (AST)} - \text{downtime}}{\text{Agreed Service Time}} * 100 \%$$

Reliability: a measure of how long a service, component or CI can perform its agreed function without interruption. It is often measured by;

$$\text{Reliability (MTBSI in hours)} = \frac{\text{Available Time in hours}}{\text{Number of Breaks}}$$

$$\text{Reliability (MTBF in hours)} = \frac{\text{Available Time in hours} - \text{Total downtime in hours}}{\text{Number of breaks}}$$

Maintainability: A measure of how quickly and effectively a service, component or CI can be stored to normal working after a failure.

$$\text{Maintainability (MTRS in hours)} = \frac{\text{Total downtime in hours}}{\text{Number of service breaks}}$$

Serviceability: the ability of a third party supplier to meet the terms of their contract.

Component Failure Impact Analysis (CFIA): Related with Capacity management and Continuity management.

CFIA defines Single point of failures (SPOF)

Fault Tree Analysis (FTA) presents which part of infrastructure; process or service cause the service interruption.

Service Failure Analysis is to define the effect of service, system or process interruption on business.

Technical Observation: Aims to define improvement opportunities in current IT infrastructure by monitoring events simultaneously.

General Information:

Table 3-14 General Information about Availability management process

Process ID	P.12
Process	Availability Management
Purpose	Availability management measure and achieve availability targets relating to the services and resources.
Scope	This process covers design, implementation, measurement, management and improvement of IT service and component availability.
Values to Business	The availability and reliability of services directly influence customer satisfaction and reputation of the business.
Inputs	Business Impact Analysis History risk trends Service Information Change and Release Information Incident management Data Financial Information Continuity Test Schedule Risk Analysis Change Schedule
Outputs	Availability Management Information System (AMIS) Availability Plan Availability and Recovery Design Criteria Service Availability, Reliability and Maintainability reports of achievements against targets An Availability Management Test Schedule The planned and preventative maintenance Schedule PSO Improvement Actions for inclusion with in SIP
Roles	Availability Manager
Tools	Reporting and analyzing tools
KPI	Percentage reduction in the unavailability of services and components Percentage increase in the reliability of services and components Percentage increase in availability of services from end to end Percentage reduction in impact and number of service interruption MTBF increase MTBSI increase MTRS reduction

Flow Chart:

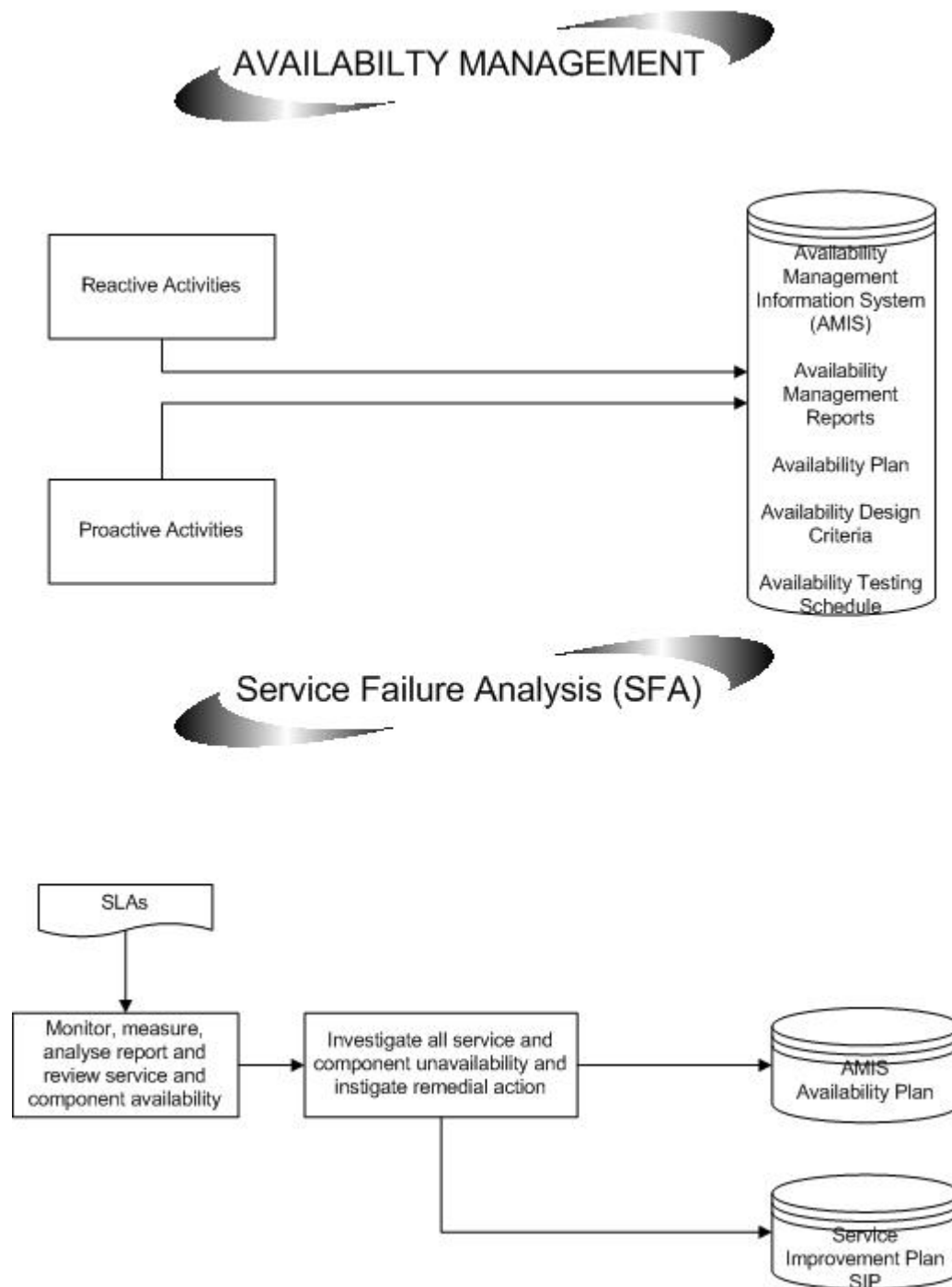


Figure 3-16 Flow chart of Availability management process

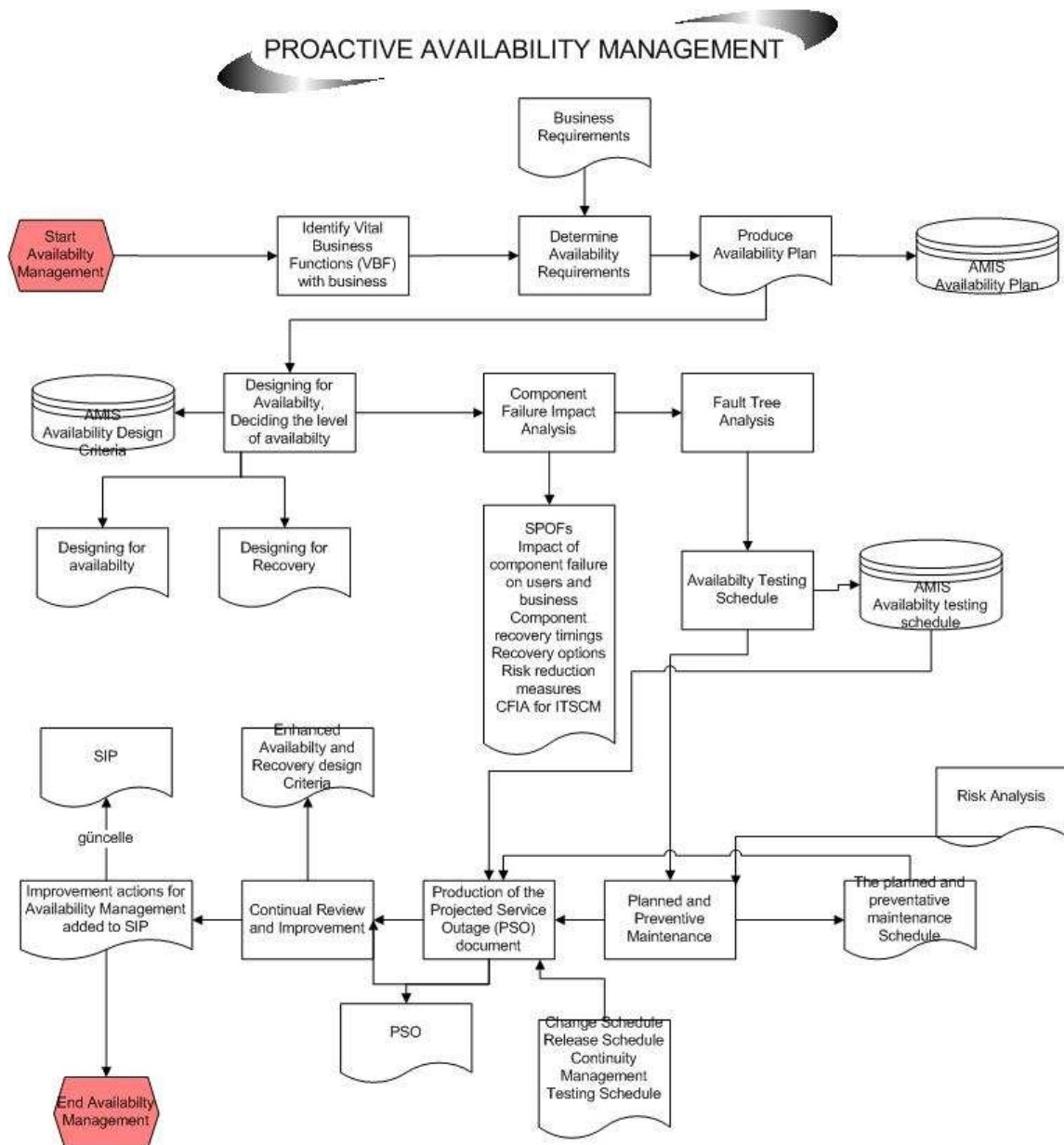


Figure 3-15 (Continued)

P.13 Event Management

Principles:

1. Decides what should be measured by considering SLM, Capacity, Availability and continuity managements.

2. There must be some responsibilities owned by defined personnel to commit event coming from event management. Otherwise, since nobody owns any event, any exception cannot be handled on time.
3. Exception does not always indicate an incident.
4. Three types of event;
 - Informational events
 - Exception events
 - Warning events

General Information:

Table 3-15 General Information about Event management process

Process ID	P.13
Process	Event Management
Purpose	Monitors all events that occur through the IT infrastructure to allow for normal operation and also detect exceptions.
Scope	It is applied to the configuration items, environmental conditions, software license, security and normal activity such as performance of a server. In short, it is applied to all service management events that must be controlled under service operation.
Values to Business	Provides mechanism for early detection of incidents. Provides more effective and efficient service management.
Inputs	Threshold, alerts and events
Outputs	Review action parameters (input for CSI) Event Information
Roles	Technical and Application Managers IT operations manager Service desk managers
Tools	Monitoring tools Event management tools provides event correlation, impact analysis and root cause analysis
KPI	Numbers of events by category Number and percentage of events that required human intervention Number of per. Events that resulted in incidents or change Number of per. Repeated or duplicated events.

Flow Chart:

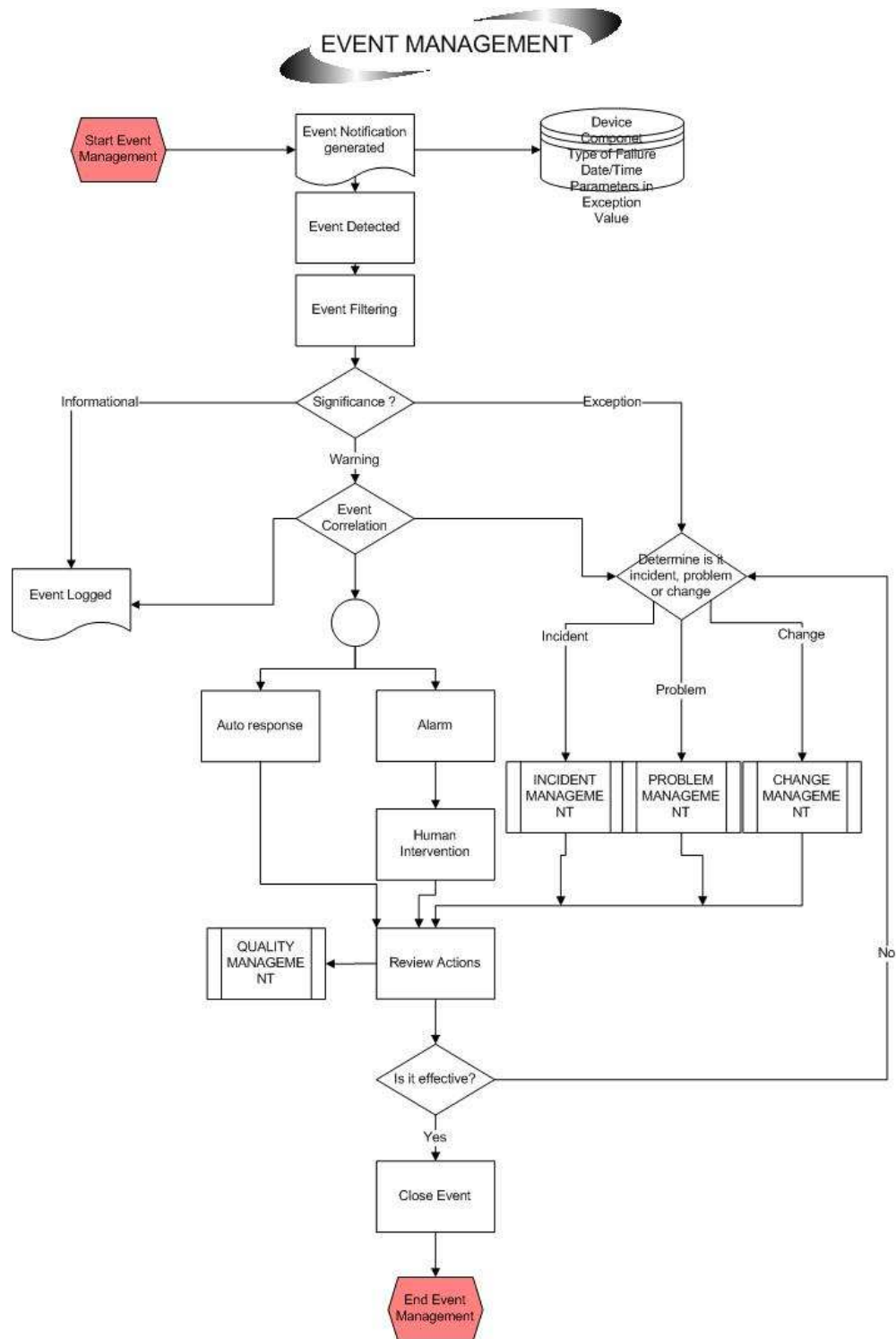


Figure 3-17 Flow chart of Event management process

P.14 Information Security Management

Principles:

1. Information security policy (ISP) and Information security management systems (ISMS) should be defined in Security Frameworks.
2. ISP should support senior IT management activities and business management activities.
3. Security policy should be known by customers.
4. Security policies should be reviewed annually.
5. Information security should be compatible with business security and business needs.
6. All IT service providers should have comprehensive information security management policy and necessary security controls.
7. Security Framework should contain;
 - ✓ Information Security Policy
 - ✓ ISMS
 - ✓ Security Strategy
 - ✓ Security Organization structure
 - ✓ A set of security controls
 - ✓ Security risks management
 - ✓ Communication strategy and plan about security
 - ✓ Training and awareness of this strategy and plan
8. Information Security policy should contain;
 - ✓ An overall Information Security Policy
 - ✓ Use and misuse of IT assets policy
 - ✓ An account and access control policy
 - Users should enter with identity verify mechanism
 - Access rights of users should be defined by adapting with business needs, documented and kept in central pool.

- Access rights are requested by users, approved by system owner and implemented by person responsible for security.
- Users identities and access rights are recorded in central pool.
- Approval mechanism should be developed for opening and closing user account.
- All user accounts and privileges should be reviewed regularly.
- ✓ A password control policy
- ✓ An e-mail policy
- ✓ An internet policy
- ✓ An anti-virus policy (For protecting technology and information systems from malicious software)
- ✓ An information classification policy
- ✓ Make security related technology resistant to tampering and do not disclose security documentation unnecessarily
- ✓ Data security policy
- ✓ A document classification policy
- ✓ A remote access policy
- ✓ A policy with regard to supplier access of IT service, information and components
- ✓ An asset disposal policy
- ✓ Network security policy (Use security techniques to authorize access and control information flows from and to networks like firewall)
- ✓ Protecting technology related to security against fire, water
- ✓ Organizing the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic to ensure the protection of keys against modification and unauthorized disclosure
- ✓ Defining a security way for transaction of sensitive data on trusted path.

General Information:

Table 3-16 General Information about Information Security management process

Process ID	P.14
Process	Information Security Management
Purpose	<p>Information should be available when required (availability), Information is on served only those who have right to know (confidentiality) Information is complete, accurate and protected (integrity) and information exchanges between enterprises or with partners can be trusted. (Authenticity and non-reputation.)</p>
Scope	<p>Production, maintenance, distribution of Information Security Policy Understanding the current and future security requirements of business Implementation of security controls Documentation of all security controls Management of suppliers and contracts in terms of access to the system in conjunction with Supplier management Management of all security breaches and incidents related to all systems and services. The proactive improvement of security controls security risk management and the reduction of security risks. Integration of security aspects within all IT SM processes. Management must establish and maintain an Information Security Management System (ISMS) to guide the development and management of a comprehensive information security programme. Testing security regularly</p>
Values to Business	<p>ISM maintains and enforced the ISP aligned with the business security policy and the requirements of corporate governance. ISM raises awareness of the need for the security with in all IT services and assets throughout the organization.</p>
Inputs	<p>Business security plans and Risk analysis IT Strategic Plan Service Information including Details of partner and suppliers Risk assessment Details of Security events and breaches from incident management and problem management Change Information Data classification Application security control conditions</p>

Table 3-16 (Continued)

Process	Information Security Management
Outputs	Information Security Management Policy ISMS A set of Security Controls Security threads and gaps Security Audits and audit reports Security Test schedules and plans Policies and processes and procedures for managing partners and suppliers and their access to services and information Security Training request
Roles	Security Manager Top Executive Manager in business and IT (Security Policy plan should be authorized.)
KPI	Percentage decrease in security breaches reported to Service Desk Percentage decrease in the impact of security breaches and incidents Percentage increase in SLA conformance to security clauses Increase in acceptance and conformance of security procedures Increased support and commitment of senior management The number of suggested improvements to security procedures and controls Decrease in the number of security non-conformance detected during audits and security testing Increased awareness of the security policy and its contents throughout the organization

Flow Chart:

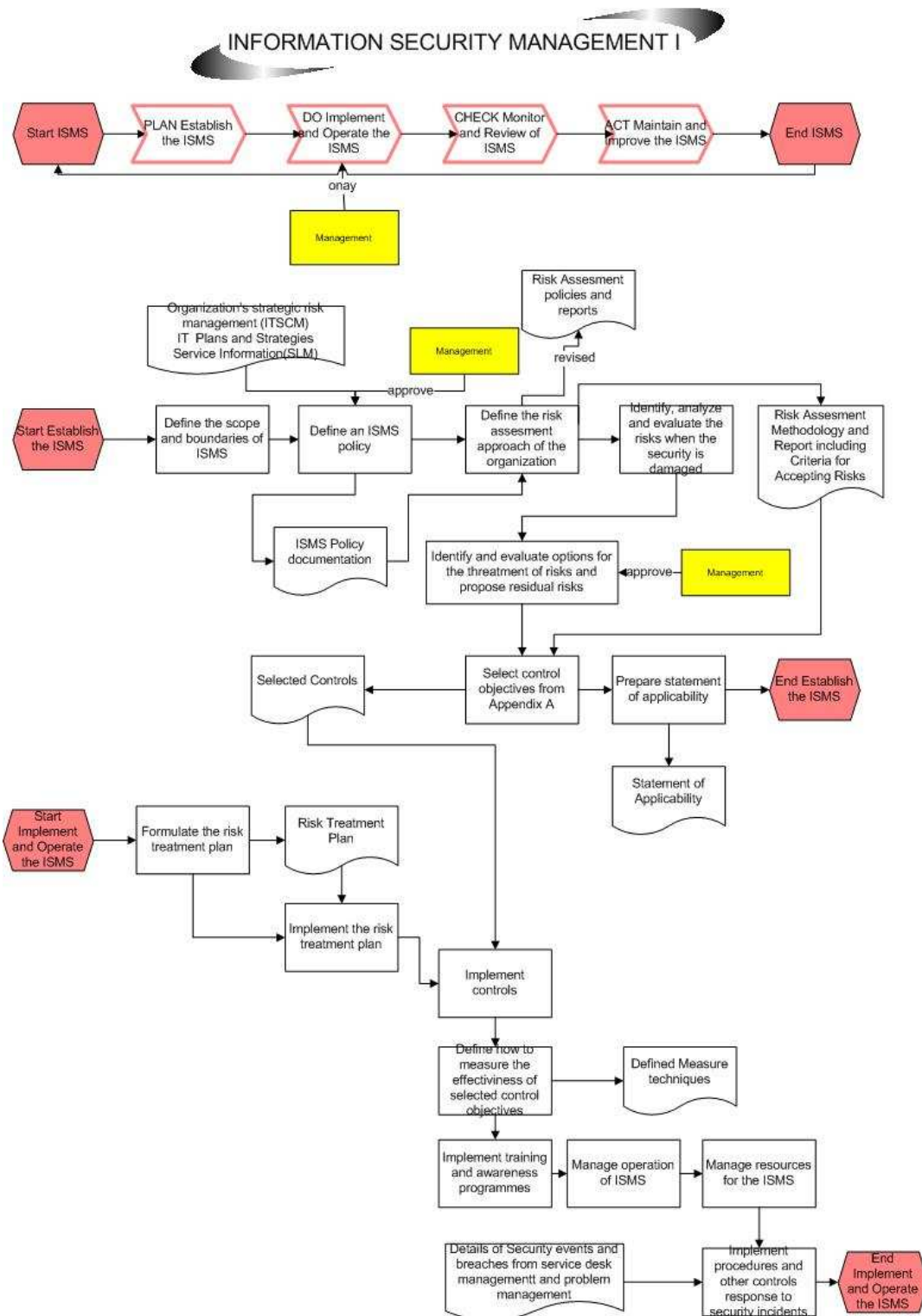


Figure 3-18 Flow chart of Information Security management process

INFORMATION SECURITY MANAGEMENT II

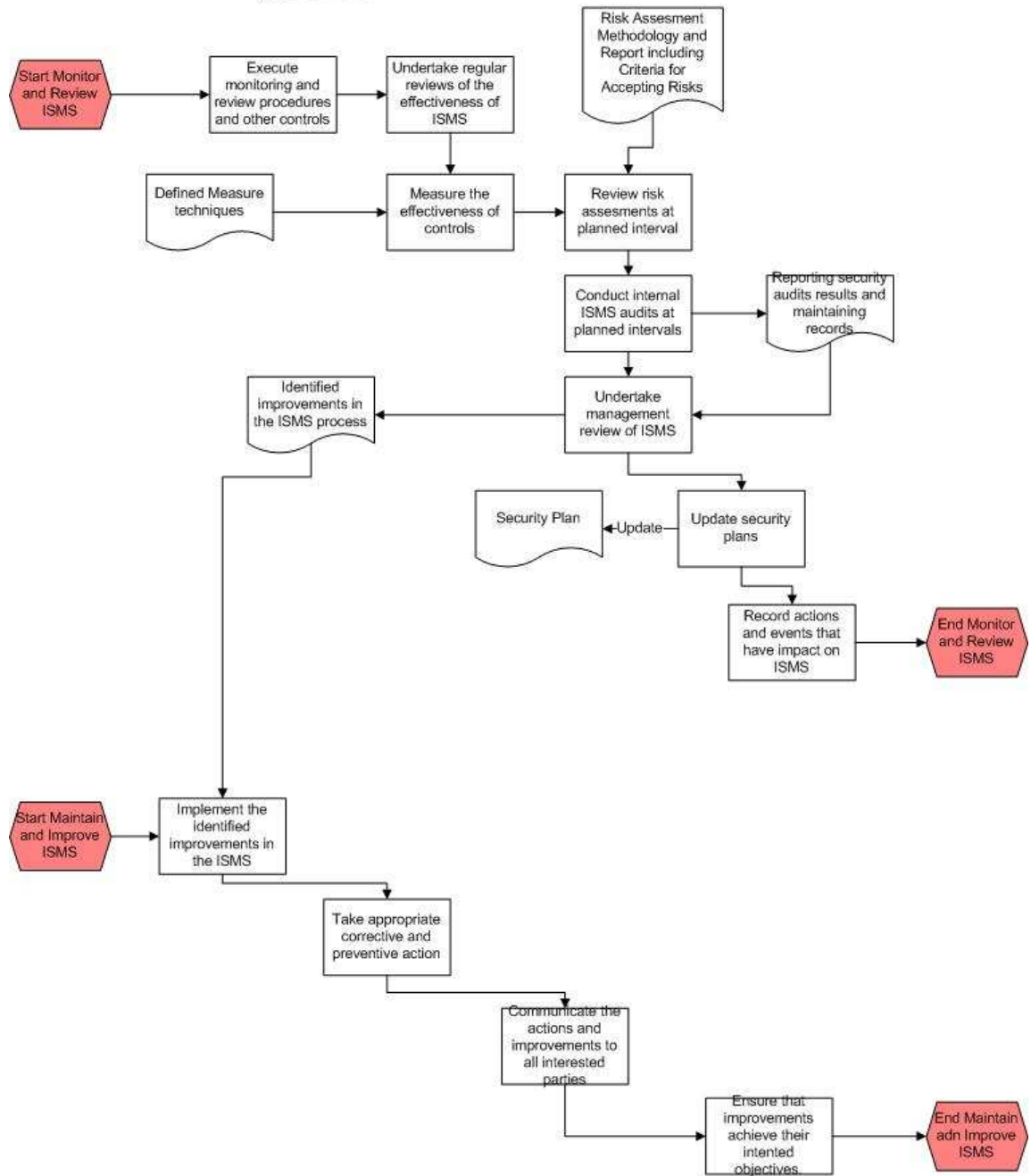


Figure 3-18 (Continued)

P.15 Supplier Management

Principles:

1. Supplier and contract database is prepared.
2. All supporting services provided by suppliers should be in Service portfolio and catalogue.
3. Agreement/contract should contain;
 - Basic conditions
 - Service definition and scope
 - Service standards
 - Workload
 - Management Information
 - Responsibilities and dependencies
4. Classification of Suppliers;
 - Strategic
 - Tactical
 - Operations
 - Commodity
5. There should be a document for each supplier. In the scope of this document, supplier roles and responsibilities, targets, expected deliveries and supplier representative credentials are included.
6. Ensuring that contracts consistent with universal business standards.
7. Supplier within the scope of risk management consider non-disclosure agreements, escrow contracts, continued supplier viability, conformance with security requirements, alternative suppliers, penalties and rewards, etc.
8. An example of Statement of Requirement is given in Appendix F.

General Information:

Table 3-17 General Information about Supplier management process

Process ID	P.15
Process	Supplier Management
Purpose	To obtain value for money from suppliers and to ensure that suppliers perform to the targets contained within their contracts and agreements, while conforming to all of the terms and conditions so that risk derived from can be minimized.
Scope	Supplier Management should include the management of all suppliers and contracts needed to support the provision of IT services to the business. The delivery to the business of end to end, seamless, quality IT services that are aligned to the business expectation. Defining a procedure and standard for sourcing
Values to Business	All targets in supplier contracts should be aligned with the business needs and agreed targets in SLAs and provide value for money from suppliers and contracts.
Inputs	Business Information Sourcing and Acquisition Strategy Financial Information Service Information CMS Business requirements feasibility study Documents Project management guideline and detailed project plan SLA Policies and processes and procedures for managing partners and suppliers and their access to services and information
Outputs	The supplier and Contracts Database (SCD) Supplier and Contract Performance information and reports and Supplier Service Improvement Plan Supplier and Contract review meeting minutes Supplier survey reports Supplier Risks Supplier Services IT Service Continuity Plans from Suppliers and partners Supplier contracts, agreements and targets
Roles	Supplier Management process owner Contracts Manager Chief Sourcing Officer

Table 3-17 (Continued)

Process	Supplier Management
KPI	<p>Increase in the number of suppliers meeting the targets within the contract</p> <p>Reduction in the number of breaches of contractual targets</p> <p>Increase in the number of service and contractual reviews held with suppliers</p> <p>Increase in the number of supplier and contractual targets aligned with SA and SLR targets</p> <p>Reduction in the number of service breaches caused by suppliers</p> <p>Reduction in the number of threatened service breaches caused by suppliers.</p> <p>Increase in the number of suppliers with nominated supplier managers</p> <p>Increase in the number of contracts with nominated contract managers.</p>

Flow Chart:

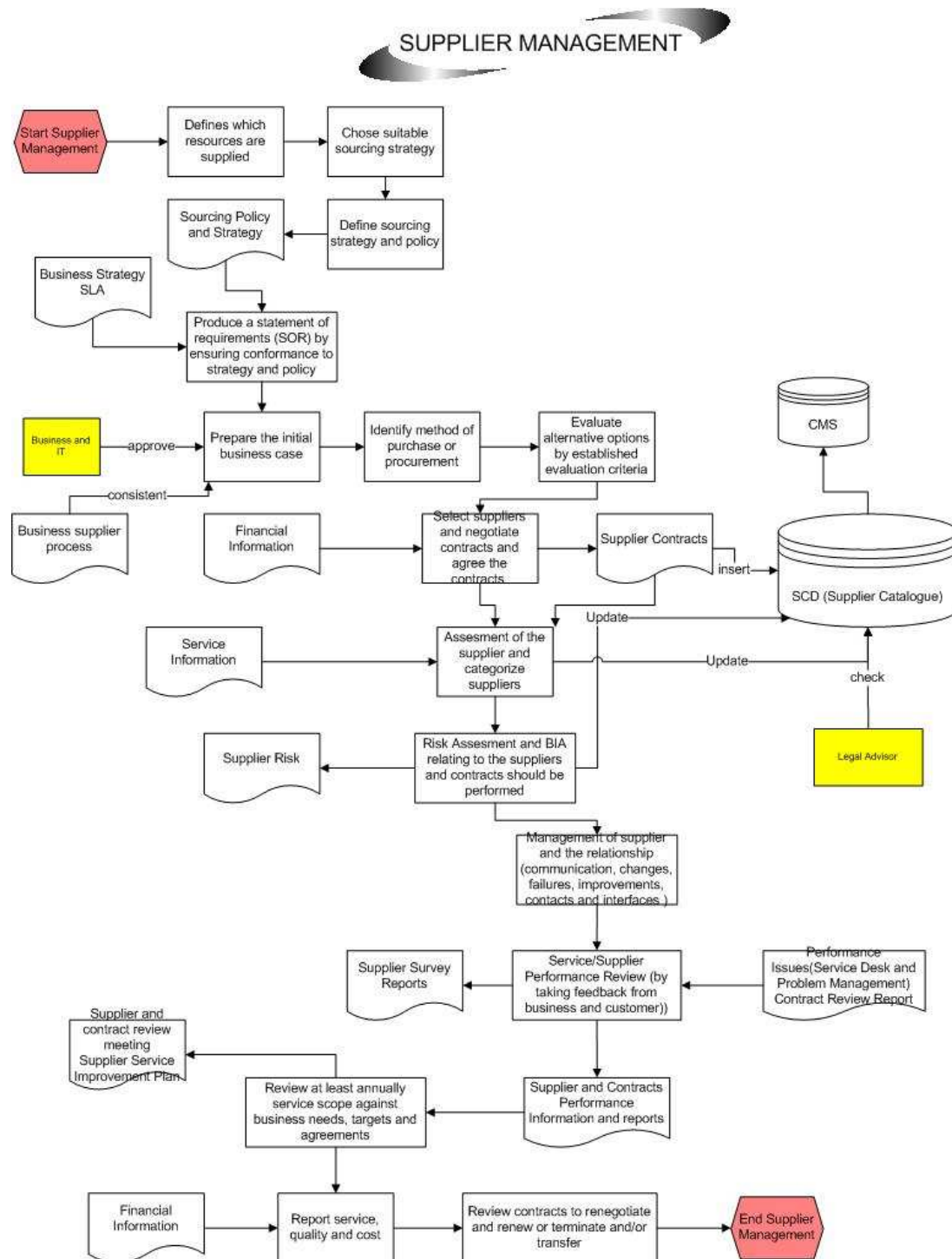


Figure 3-19 Flow chart of Supplier management process

P.16 Human Resources Management

Principles:

1. Reviewing of role and responsibilities depends on sensitive of roles.
2. While defining training needs, the followings are regarded;
 - Current and future business needs and strategy
 - Evaluate information as an asset
 - Organization values like ethical, control, security culture
 - New IT infrastructure or software implementation
 - Current and future skills
 - Education presentation methods

General Information:

Table 3-18 General Information about Human Resources management process

Process ID	P.16
Process	Human Resources Management
Purpose	Recruitment and training of IT personnel, providing motivation on her/his career, appointed to roles suitable her/his skills and defining job definitions
Scope	Review of personnel performance Provide recruitment and training IT personnel Reducing risks because of extreme dependencies on key resources
Values to Business	Acquiring motivated and competent personnel to define and deliver IT services Defining effective training strategy by understanding user training needs and measuring results

Table 3-18 (Continued)

Process	Human Resources Management
Activities & Tasks	<p>Designing database contains skills, trainings, courses and seminars that attends or gives, historic job information and education of IT personnel</p> <p>Defining IT skills, position definitions, salary interval and personnel performance benchmarks</p> <p>Recruitment and protection of IT personnel processes should be compatible with organization personnel policy and procedure</p> <p>Defining requirements of IT principal competence, verifying that competence is protected</p> <p>Verifying convenience of personnel capability to their jobs regularly</p> <p>Monitor and manage roles, responsibilities and compensation of personnel frameworks</p> <p>Provide training to increase capability of IT personnel</p> <p>Decide and define training needs of personnel</p> <p>Choosing target groups and members according to the defined training</p> <p>Assigning necessary instructor, trainer or mentors to the training according to the needs of trainings</p> <p>Recording attendances</p> <p>Evaluate context of training in terms of relevancy, quality, effectiveness, retention of knowledge, cost and value (important input for deciding future training need)</p> <p>Reducing dependencies on only one personnel by assigning a more new personnel to key personnel or making written key personnel knowledge</p> <p>Reviewing background of IT personnel in IT recruitment process and after that regularly depending on the sensitive and criticality of the function of job</p> <p>Evaluate job performance of employees periodically</p> <p>Taking expedient actions regarding job changes, especially job terminations(Removing access rights, reassigning responsibilities, knowledge transfer, guarantying continuity of functions)</p>
Inputs	<p>Documented roles and responsibilities</p> <p>Business requirements feasibility study</p> <p>Security training request</p> <p>Training materials (Knowledge management)</p> <p>Knowledge transition requirements</p>

Table 3-18 (Continued)

Process	Human Resources Management
Outputs	IT human resources policy Skills inventory Job Descriptions Users capabilities
Roles	HR Manager
KPI	Percent of employees trained Percentage of IT staff members corresponding to competency profile Percent of IT roles filled Percent of stakeholder satisfaction with training provided Percent of working days lost due to unplanned absence Percent of IT staff members who complete annual IT training plans Actual ratio of contactors to personnel vs. planned ratio Percent of IT employees who have undergone background checks Percent of IT roles with qualified backup personnel

Flow Chart:

There exists no flow chart for this process.

P.17 Project Management

Principles:

1. Project and programme framework provides prioritization and coordination of projects. This framework contains basic plan, assigning resources, definitions of deliverables, approval of users, quality assurance, test plan and revision after implementation.
2. Project approach should be defined according to project size, complexity and regulatory requirements.
3. Project governance structure should include roles and responsibilities, project sponsor, management committee, project office and project manager.
4. Project Plan contains;

- ✓ Documenting relationship with other projects if exists.
- ✓ Risk Plan (elimination or mitigation risks with systematic processes for planning, analyzing, responding, monitoring and controlling of events that cause undesirable changes
- ✓ Test Plan
- ✓ Cost Plan
- ✓ Resource Plan (defining roles, responsibilities, authorities and performance criteria of project group members, planning acquisition of product and services for each project)
- ✓ Monitoring Plan
- ✓ Supplier Plan
- ✓ Quality Assurance Plan (This plan should be approved by all related people)
- ✓ Release and Deployment Plan

General Information:

Table 3-19 General Information about Project management process

Process ID	P.17
Process	Project Management
Purpose	Identify project and programme management approach to manage projects and provide participation of stakeholders to monitor project and risks.
Scope	Define program and project framework and approach Publish project management guideline Prepare detail project management plan for each project in project portfolio
Values to Business	Finish projects on time, budget and qualified
Inputs	Project Charter Project Portfolio Development Standards Skills Inventory
Outputs	Project management guideline Project plan Project risk management plan Project performance report Lessons Learned Initial Planned SLA and OLA
Roles	Project manager Project team
Tools	Project management tools
KPI	Percentage of project suitable with project management standards Number of changes on project Effect of changes on project manpower and time Percentage of project schedule deviation Percentage of project effort deviation – Manpower performance Percentage of project budget deviation – Budget performance Number of incidents during early lifecycle

Flow Chart:

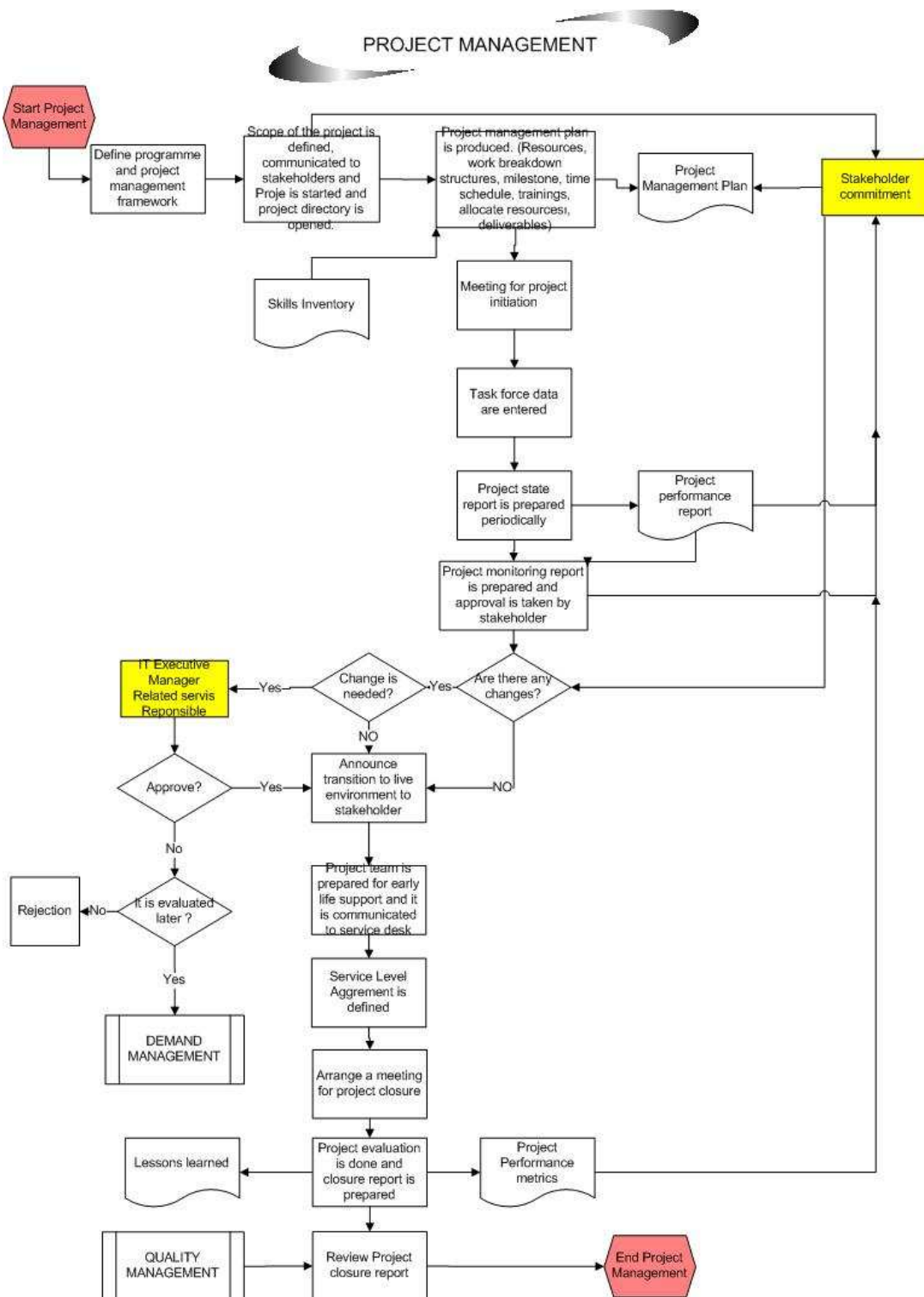


Figure 3-20 Flow chart of Project management process

P.18 Change Management

Principles:

1. To increase success of changes, management's support is needed.
2. Change is both proactive (improve services) and reactive (solve errors).
3. During this process, changes' effect on risk and business continuity, analyzing of changes, resource needs, whether achievable business value is created or not is evaluated.
4. Emergency changes can be operable by different authorization.
5. Post Implementation Review: After accomplishing changes, if improvement becomes unsuccessful, improvement continues.

Policies;

- ✓ Defining change management policy, rule and procedure
- ✓ Reduction of unauthorized changes to zero
- ✓ Aligning change management procedure with shareholder, business and project change management procedures
- ✓ Prioritize changes
- ✓ Define responsible for all changes
- ✓ Achieving risk assessment and measuring performance of change management
- ✓ Integrating change management with other service management processes to watch change
- ✓ Defining and classifying change document
- ✓ Defining change document type and template
- ✓ Defining organizational roles and responsibilities
- ✓ Grouping or associating related changes
- ✓ Not approving changes that does not have recovery plan

Differences of emergency changes from standard changes;

- ✓ Change approve is also compulsory but this approve can be taken by Emergency Change Advisor Board (ECAB).

- ✓ Test cases can be reduced even they cannot be done at extreme cases.
- ✓ Change recordings can be done after implementation change. (update RFC and Configuration data)

General Information:

Table 3-20 General Information about Change management process

Process ID	P.18
Process	Change Management
Purpose	Standardized methods and procedures are used for efficient and prompt handling of all changes All changes to service assets and configuration items are recorded in the Configuration Management System Overall risk business is optimized
Scope	It covers the all changes to baseline service assets and configuration items across the whole service lifecycle. It is divided into three parts ; Strategic Change, Tactical Change and Operational Change
Values to Business	Reliability and business continuity is important for business success. Service or infrastructure changes can have a negative impact due to service disruption and delay in identifying business requirements but Change management overcome this situation
Inputs	Change Proposals Request for Change Project Plan Current Change Schedule and PSO CMS Configuration baseline Evaluation Plan Test results, test reports and Evaluation Report Completed RFC
Outputs	Rejected RFC Approved RFC Change to services New, changed or disposed assets or configuration items Change Schedule Authorized Change Plan Change decisions and actions Change documents and reports / Reports of Change Monitoring Change Information Change Evaluation

Table 3-20 (Continued)

Process	Change Management
Roles	CAB members Managers and Executives Change Manager
Tools	Integrated service management tool Change Schedule and projected service availability can be automated Risk assessment and prioritization can also be automated Linkage of incidents, problems, changes and releases should be done
KPI	Number of disruptions, incidents, problems/errors caused by unsuccessful changes and releases Inaccurate change specifications Incomplete impact assessment Unauthorized business/customer change by business/IT/customer/user asset of CI type. Percentage reduction in time, effort, cost, to make changes and releases Percentage improvement in predictions for time, quality, cost, risk, resource and commercial impact Percentage improvement in impact analysis and scheduling of changes safely, efficiently and effectively reduces the risk of changes affecting the live environment Percentage reduction in unauthorized changes Frequency of change Volume of change People's satisfaction with the speed, clarity, ease of use Number and percentage of changes that follow formal change procedure Ratio of planned vs. unplanned changes Ratio of accepted or rejected change requests

Flow Chart:

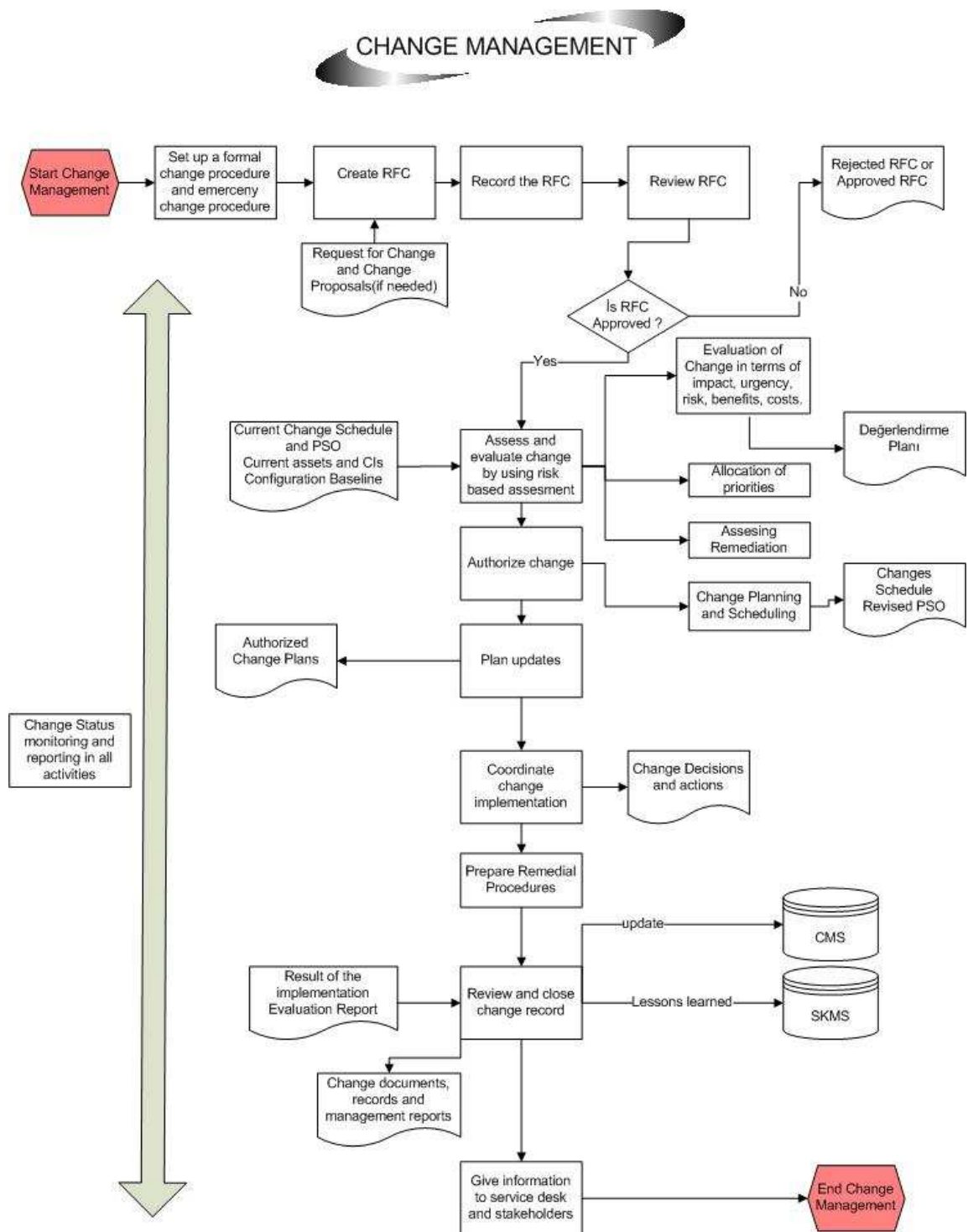


Figure 3-21 Flow chart of Change management process

Change Authorization Model

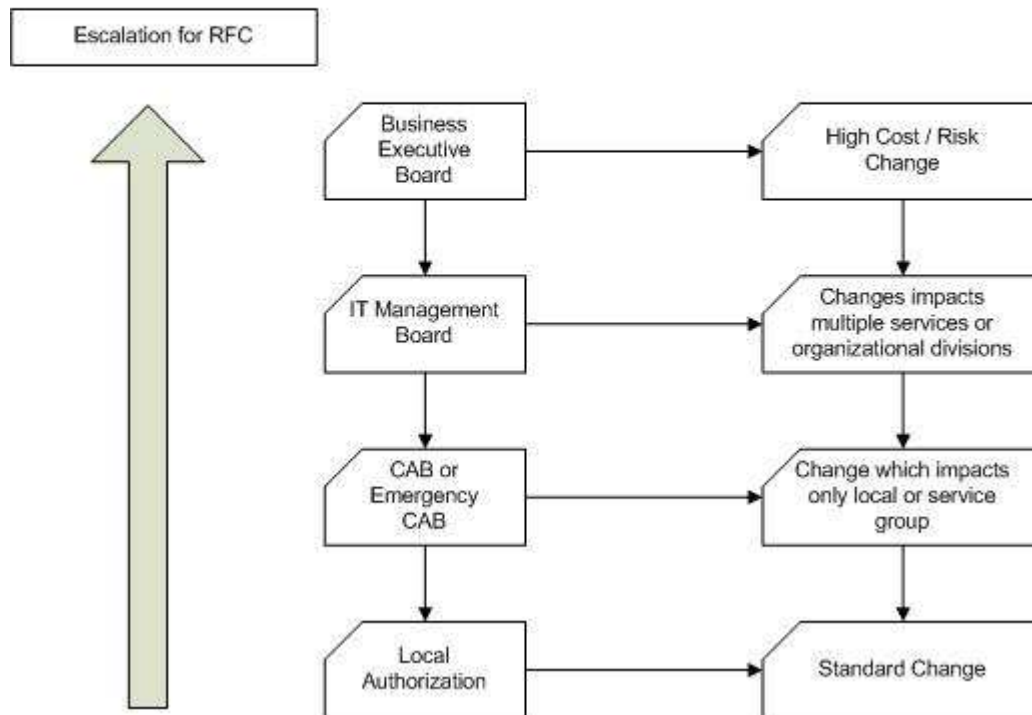


Figure 3-22 Change Authorization Model

P.19 Release and Deployment Management

Principles:

Release Unit is the part released in conformity with release policy of Service or IT infrastructure organization.

The content of Service Design Package (SDP) is given in Appendix A.

Policies;

1. Deciding the most appropriate release unit level

2. Deciding definition of release unit such as Configuration item (CI) definition
(Decide the release unit identification similar to the CI identification)
3. Deciding release design options (‘Big bang’ vs. phased, push vs. pull and automation vs. manual)
4. Designing release and release packets (Which sub-deployments first installed and relationship between sub-deployments)
5. Frequency and type of release
6. Automation of building, construction, release distribution process in suitable cases
7. Determining configuration baseline for release
8. Forming input and output criteria for acceptance of Release during each service transition phase
9. Determining criteria and authorizations for completing early life support phase
10. Data transformation and infrastructure replacements should be planned within recovery plan.
11. Planning release packaging and build contains;
 - Scope and content of release
 - Risk assessment for release
 - Stakeholders being affected from release
 - Stakeholders approving modification change request for release
 - Team in charge with release
12. Deployment planning contains;
 - Confirmation of input and output criteria
 - Managing communication and change with stakeholders
 - Training persons and transferring information
 - Establishing service and service assets
 - Deciding on schedule
 - Converting system and users from existing application and technology to new or changing services

- Developing competence and sourcing of service management
- Evaluating availability of target transfer groups for release (customer, user, service operation personnel)
- Agreeing upon output criteria

13. While releasing build and test, the followings should be done;

- Management of configuration
- Utilization of build and test environments
- Preparation of release documentation
- Receiving and testing input CI and components
- Releasing packet

Prepare for Service Transition;

1. Acceptance and revision of inputs required for transition
2. Completion of Change requests forms
3. Controlling of configuration baseline is recorded prior to starting service transition

Early Life Support:

1. Deployment teams apply improvements and rapidly solve all problems.
2. It frequently updates Documents and Knowledge databases with diagnosis, known errors and workarounds.
3. Monitoring the support of early life continuously until output criterion is provided.

General Information:

Table 3-21 General Information about Release and Deployment management process

Process ID	P.19
Process	Release and Deployment Management
Purpose	<p>Plan appropriate capacity and resources to package a build, release, test, deploy and establish the new or changed service into production</p> <p>Provide support for the Service Transition Teams and people</p> <p>Ensure that integrity of all identified customer assets, service assets, and configurations can be maintained through Service Transition</p> <p>Ensure that service transition issues, risks and deviations are reported to the appropriate stakeholders and decision makers</p> <p>Define release and deployment plans</p> <p>Ensure that all release and deployment packages can be tracked, installed, tested and verified or back out, uninstalled</p> <p>Record and manage deviations, risks, issues related to the new or change service and take corrective action</p> <p>Ensure that knowledge and skill is transferred to users and customers to support use of their business Activities and operations and support staff to enable them to effectively and efficiently deliver, support and maintain service.</p>
Scope	Release and deployment management packages, builds, tests and deploys a package into production and establish the service specified in service design package before final handover to service operations.
Values to Business	<p>Well planned and implemented release and deployment reduces the its cost significantly.</p> <p>Increase the ability of service provider in terms of the handling high volumes of change and releases across its customer base</p>
Inputs	<p>Authorized RFC</p> <p>SDP</p> <p>IT service continuity plan</p> <p>Technology and procurement standards</p> <p>Scripts used before and after deployment</p> <p>Scripts necessary for controlling software and hardware configurations before and after deployment</p>

Table 3-21 (Continued)

Process	Release and Deployment Management
Outputs	Release and deployment plan Completed RFC Updated Service Catalogue New or changes Service Management documentation New or changed service reports Service Capacity Plan Released Configuration Items Service Transition Report Evaluation Report Transition Strategy Integrated set of Service Transition Plans Environments requirements and specification for test Release Information
Roles	Service Transition Manager The release and deployment manager The release packaging and build manager Deployment staff Early life support staff
KPI	Variance from service performance required by customers Number of incidents against the service Increased customer or user satisfaction Decreased customer dissatisfaction Reduced resources and costs to diagnose and fix incidents and problems in deployment and production Increased adoption of the service transition common framework of standards , re-usable processes and supporting documentation Reduced discrepancies in configuration audits with the real world

Flow Chart:

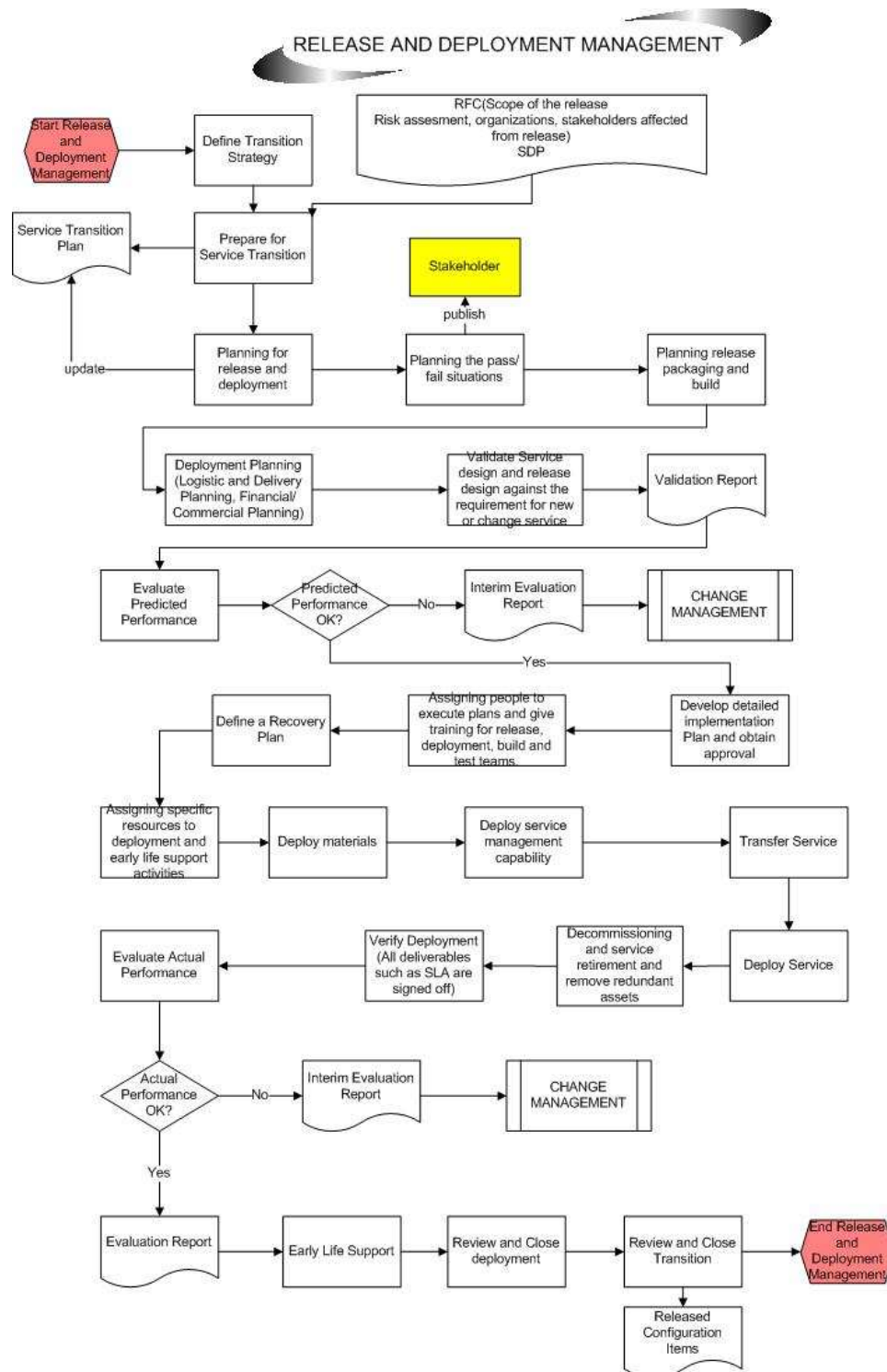


Figure 3-23 Flow chart of Release and Deployment management process

P.20 Test Management

Principles:

1. Service validation and verification is playing an important role in service management. It is the reason of effectiveness of service management processes.
2. Service design package (SDP) and software development business requirements are the key inputs for test management.
3. During test process, whether constraints on design is defined accurate or not is controlled.
4. Test Strategy;
 - ✓ Translating service requirements into test requirements and test models.
 - ✓ Translating service acceptance criteria into input and output criteria for each level of test.
 - ✓ Translating events and risks into test requirements.
5. Test Models;
 - ✓ Test models contain test plans (what is tested) and test scripts (how each element is tested).
 - ✓ It is tested by different perspectives (business, service provider, user, operation and service improvement)
6. Test Types;
 - ✓ Usability testing
 - ✓ Accessibility testing
 - ✓ Process and procedure testing
 - ✓ Knowledge transfer and competence testing
 - ✓ Performance, capacity and resilience testing
 - ✓ Volume, stress, load and scalability testing
 - ✓ Availability testing
 - ✓ Backup and recovery testing
 - ✓ Coherency testing
 - ✓ Compatibility testing

- ✓ Documentation testing
- ✓ Regulatory and compliance testing
- ✓ Security testing

Policies;

With service quality, risk, and release and deployment management policy:

1. Publishing re usable policy containing test library, test models, test cases, test scripts and test data
2. Combining test with project and service lifecycle
3. Adapting risk based approach
4. Communicate with customer, shareholder, user and service teams for capability of testing and feedback about the service and service assets of them
5. Automate testing by using automatic test tools and systems

General Information:

Table 3-22 General Information about Test management process

Process ID	P.20
Process	Test Management
Purpose	Plan and implement a structured validation and test process that provides objective evidence that the new or changed service will support the customer's business and stakeholder requirements, including the agreed service levels.
Scope	Testing is applicable equally in house or developed services, hardware, software and knowledge based services. It includes the testing of new or changed services and service components and examines the behavior of these in the target business unit, service unit, deployment group or environment.
Values to Business	Service failures because of the low testing result in outcomes such as loss of reputation, loss of money, loss of time, injury and death. The key value to the business and customers from Service validation and testing is in terms of the established degree of confidence that a new or changed service will deliver the value and outcomes required of it and understanding the risks.
Inputs	Service Design Package Release and Deployment Plans Approved RFC Environments requirements and specification for test
Outputs	Configuration baseline Test results, test reports and Evaluation Report Known and accepted errors Test incidents, problems and error records Improvement ideas for Continual Service Improvement
Roles	Service test manager Test support Build and test environment staff
Tools	Automated Test Tools
KPI	Understanding the different stakeholder perspectives that underpin effective risk management Issues are identified early in the service lifecycle.

Flow Chart:

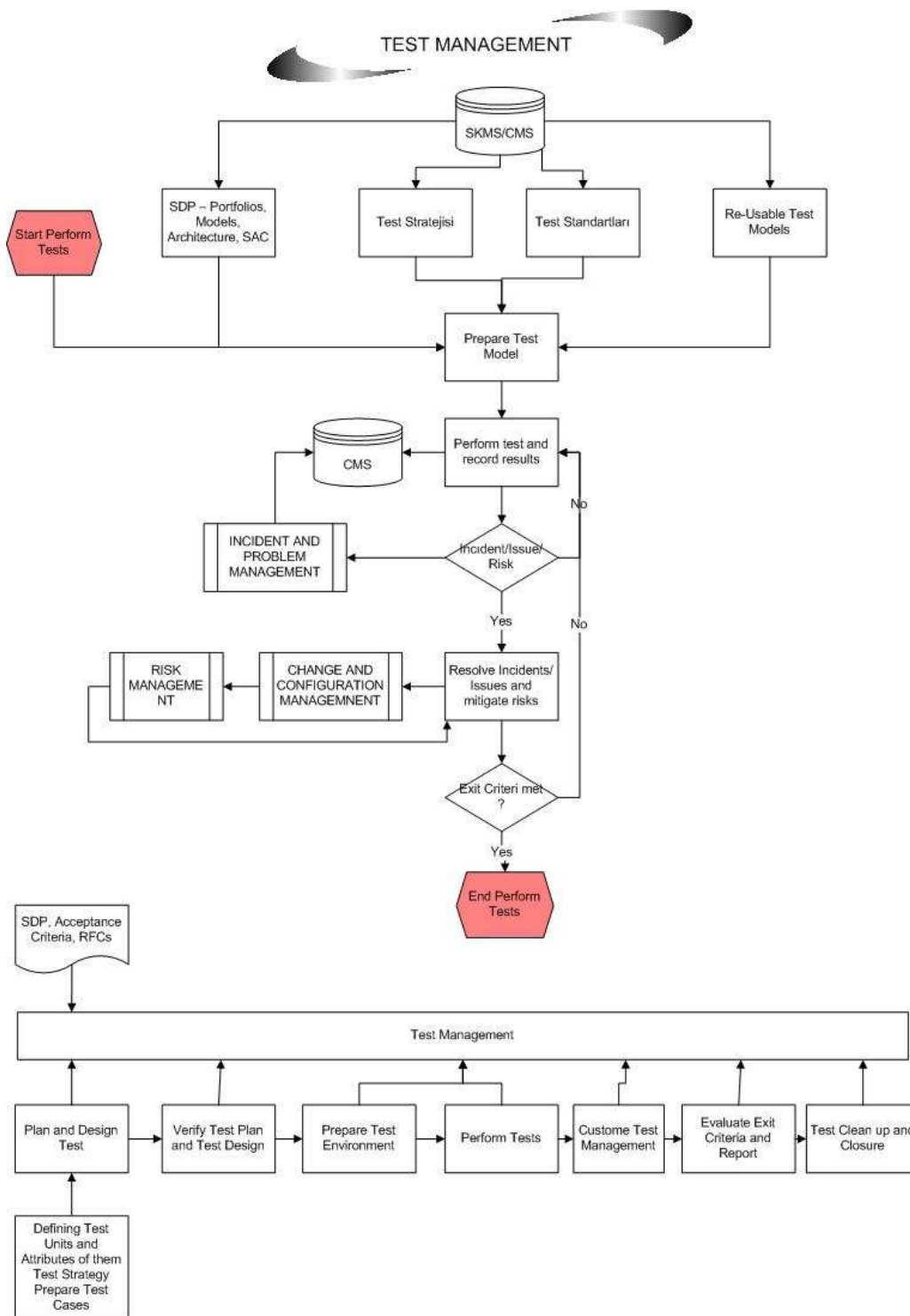


Figure 3-24 Flow chart of Test management process

P.21 Knowledge Management

Principles:

This process target is to increase decision quality by providing secure and reliable information, problem solving, dynamic learning and strategic planning.

1. The data – to – Information – to – Knowledge – to – Wisdom (DIKW) is based.
2. Service Knowledge Management System contains;
 - a. Personnel skill information
 - b. Number of users, organization performance shapes
 - c. Needs and expectations of suppliers and shareholders
 - d. User skill level
3. Knowledge Transfer types; Learning styles, knowledge visualization, Driving behavior, seminars, webinars and advertising , Journals or newsletters
4. Information Architecture is defined by;
 - Modeling in a way that creation, using and sharing of information shall be cost-effective, on time and flexible.
 - Protecting data and information integrity while using information
 - Adopting data classification chart to be used within whole organization
5. Information sharing should be delivered to users, stakeholders, customers and personnel by providing not only documentation but also the training at the same time.
6. Each data required to be processed is gathered and is processed accurately and on time. Gathered data is presented according to work requirements.
7. Determining and implementing procedure for storing, preserving and archiving of data in a way that shall meet work requirements in conformity with information security policy.
8. Determining and implementing an active procedure for media maintenance recorded and archived for providing usability and integrity.

9. When data and equipment are transferred or disposed of, completing and implementing procedure for providing satisfaction of work requirements required for protection of sensitive data and software.

Data policies;

1. All users should access all information which they are entitled to access on time whenever they desire
2. Data of organization should be able to be protected in an acceptable level and information should be accurate, reliable and consistent
3. Safety, integration and confidentiality of data should be protected with prohibited requirements
4. Forming an efficient procedure for storing, protecting and archiving data
5. Completing and implementing a procedure for maintenance of stored and archived media inventory
6. Completing and implementing a procedure for protecting sensitive data and software when data or equipment is disposed of or is transferred to another equipment
7. There should be relationship between software applications and presented services
8. It should be decided on application framework for software applications
9. Establishing efficiency and control in information sharing between applications
10. A tool intended for recording versions for software applications should be supplied.
11. Application developers develop software by using framework which architectural developers or application framework developers develop by focusing on requirement of work.
12. A compatible order should be determined for coding. In other words, coding style should be performed under specific standards.
13. There should be readily-prepared templates for creating components of general application.
14. There are two fundamental elements for a successful information management;

- a. Open Culture: The act of rewarding and being enthusiastic to learn due to the fact information which everyone has is shared.
- b. Infrastructure: Preparation and implementation of required infrastructure of information sharing.

General Information:

Table 3-23 General Information about Knowledge management process

Process ID	P.21
Process	Knowledge Management
Purpose	Knowledge is delivered to the appropriate place or content person at the right time so, decision making phase becomes very effective. It provides completeness, accuracy, availability and protection of data.
Scope	Data resources, data and information technology, information process and data standards and policies are managed. Configuration and asset data is set out. Defining information architecture
Values to Business	Simplification of user, service desk, support staff and supplier responsibilities by accessing known errors of new or changed services Increases the awareness of services' usage Providing information when needed and optimizing usage of information
Inputs	Project management guideline and detailed Project plans Business requirements feasibility study Application and Package software knowledge IT Infrastructure information Known and accepted errors / Problem record Backup storage and protection plan
Outputs	Whole processes, people needed defined in Knowledge management strategy. Knowledge transition requirements Training materials Data management guideline Data dictionary / data classification schema
Roles	Knowledge management process owner

Table 3-23 (Continued)

Process	Knowledge Management
Tools	Document Management Tools Records Management Tools Content Management Tools (Version Control, Document Architectures) KMS capture data through incident and problem management
KPI	Frequency of updates done on organization data model Percentage of data which has not owner Frequency of data verification activities Level of participation of user groups Percentage of incidents results from deficiencies of user and operation document and training Decrease in the cost preparing training materials, user documents and operation procedures Number of training calls handled by service desk Percentage of successful data restore Number of data integrity incidents or downtime because of insufficient storage capacity After disposal of medias, incidents about the transition of sensitive data

Flow Chart:

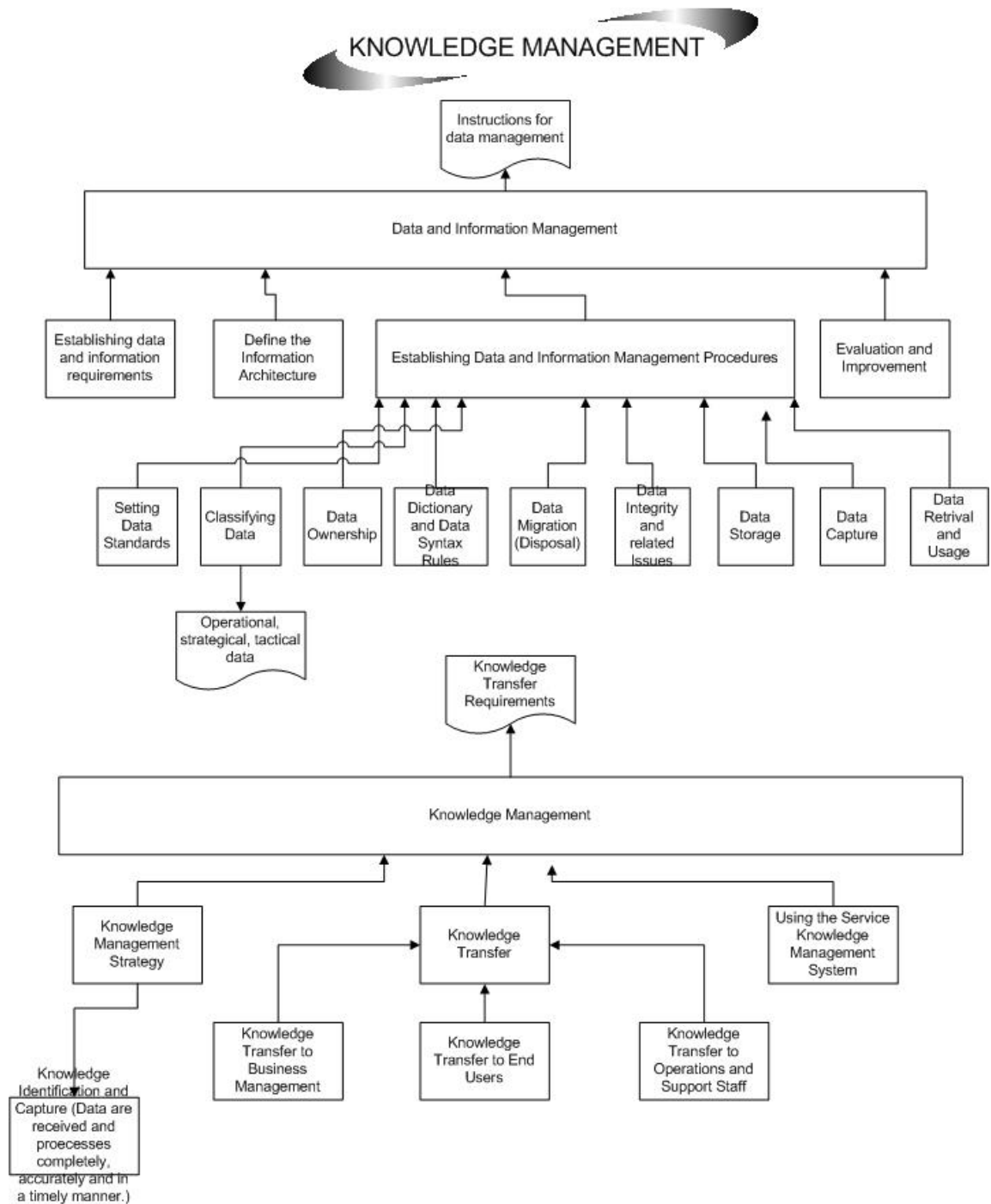


Figure 3-25 Flow chart of Knowledge management process

P.22 Request management

Principles:

1. It is the process evaluating the requests received from customer and managing and fulfilling them accordingly.
2. It evaluates the request received regarding access rights. It considers the policy and actions created under the management of Security while performing evaluation process.
3. Requests may be created similarly with previous requests like event models or there may be encountered with the requests in identical nature. Afterwards, standard realization steps are determined for frequently-repeated requests and consecutively the same type requests are fulfilled according to determined standard.

General Information:

Table 3-24 General Information about Request management process

Process ID	P.22
Process	Request Management
Purpose	Involves the management of customer or user requests that are not generated as an incident from an unexpected service delay or disruption. Granting authorized users the right to use a service, while restricting access to non-authorized users.
Scope	Incoming requests are investigated by first line/second line/third line and contains some task to realize requests.
Values to Business	Fulfillment of customer request fast and effectively by minimizing bureaucracy Increase the customer satisfaction in addition to the quality of request fulfillment
Inputs	Request form containing information needed from customer Agreed service request from Service portfolio Access rights in Security Policies CMS
Outputs	RFC (update CMDB if needed)
Roles	Service desk manager Service desk supervisor Service desk analyst Super users Technical manager Technical analyst Technical operator Incident manager IT operations manager
Tools	Portal providing users to request services Workflow engine provides manage request and capture related cost Access rights management tool (Human resources management tool, Directory Services Technology or Request Fulfillment technology)
KPI	Total number of service request Breakdown of service requests at each stage The mean elapsed time for handling each type of Service Requests Number of request for access Number of incidents caused by incorrect access settings

Flow Chart:

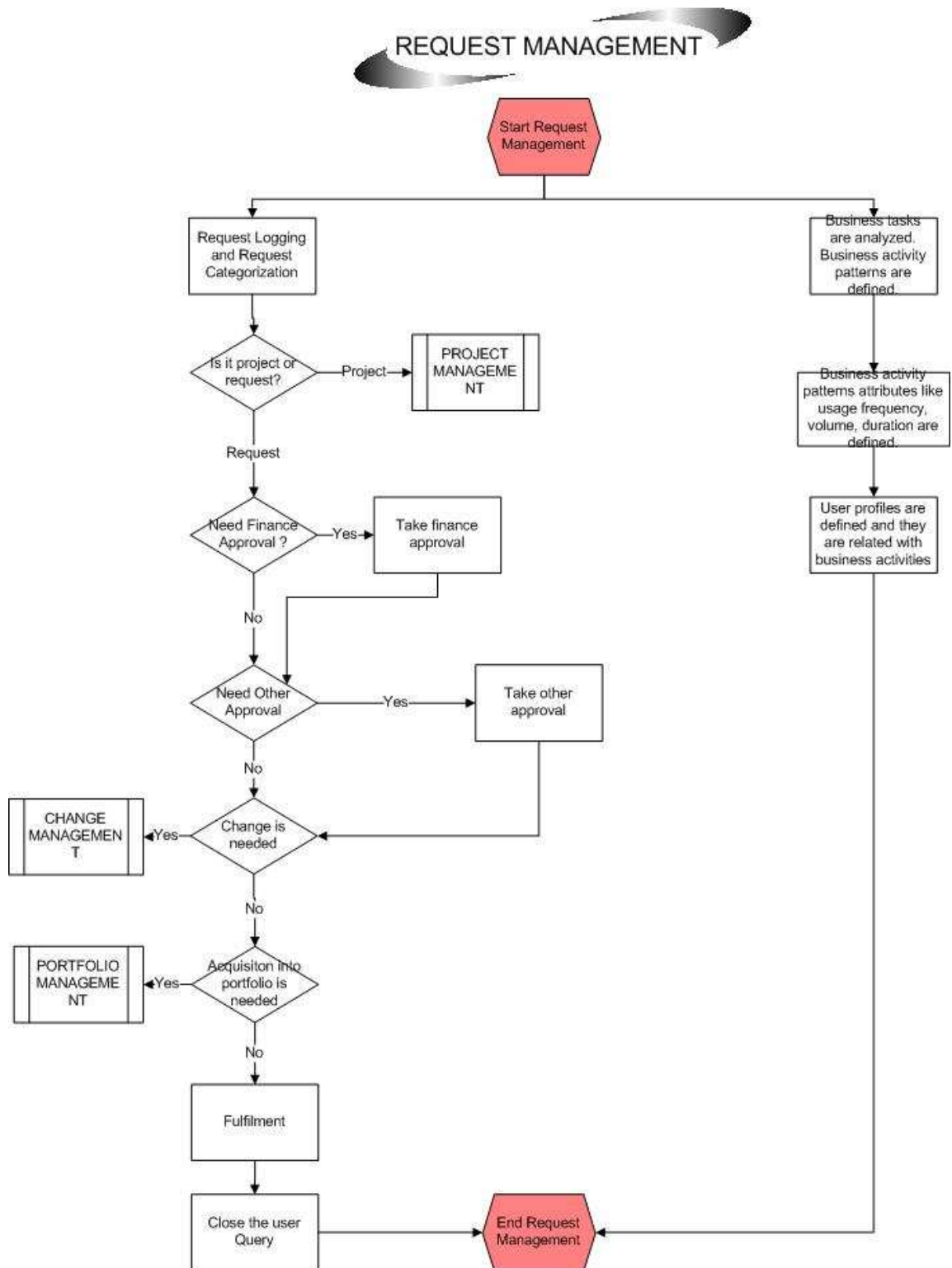


Figure 3-26 Flow chart of Request management process

P.23 Incident Management

Principles:

1. Definition of Incident is that “Unplanned interruption to an IT service or reduction in the quality of an IT service” [36].
2. Incident management is related to all incidents.
3. Incident management defines steps before for standard incidents. By this way, similar incidents occurs, pre defined way is followed.
4. Service desk ensures that all activities are recorded and users are informed about process.
5. Classification in incidents is significant.
6. “Investigation and Diagnosis” and “Resolution and Recovery” is done simultaneously because of time restriction.
7. The phase of incident is always updated so person who opens the incident can trace the incident.
8. Define clear escalation criteria and procedure

General Information:

Table 3-25 General Information about Incident management process

Process ID	P.23
Process	Incident Management
Purpose	Focusing on restoring the service as quickly as possible
Scope	Includes any event which disrupts or could disrupt a service
Values to Business	Increase the service availability by noticing and solving incidents Identify necessary services and training requirements for service desk
Inputs	CMDB in CMS Known and accepted problems/errors Security incidents Scripts which are necessary to start and stop application SLA PSO Authorized Change Plan Event Information

Table 3-25 (Continued)

Process	Incident Management
Outputs	Incident information forms RFC Service Performance Information Incident management data Incident response times, impact definitions for SLM Customer and User Feedback Details of Security events and breaches from incident management
Roles	Incident Manager First line Second line Third line (Suppliers, hardware manufacturers,...)
Tools	Incident management tools Service desk tool Incident solving tools defined previously Integrated CMS and KEDB Reporting Tools
KPI	Total number of incidents Breakdown of incidents at each stage Size of current incident backlog Number and percentage of major incidents Average cost per incident Ratio of solving incident on service desk (first line) Reopen incident ratio Average of turn back to request comes from telephone or e-mail Percentage of incident withdraw Average time of major incident

Flow Chart:

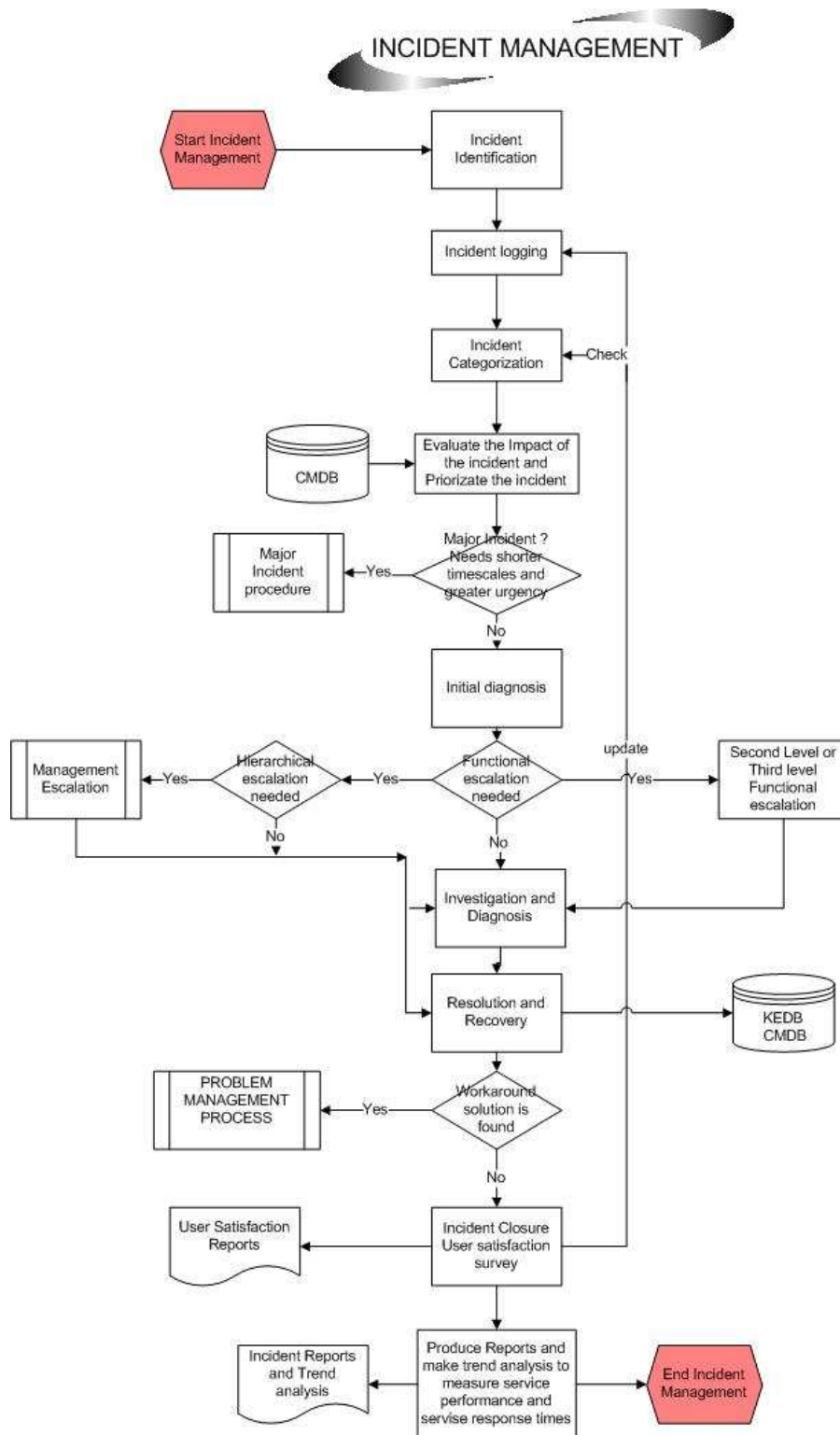


Figure 3-27 Flow chart of Incident management process

P.24 Problem Management

Principles:

1. Problem management has a powerful relationship with knowledge management. Both of them using the known error database.
2. Problem management has reactive and proactive processes.
3. A difference of problem than incident is to find root cause. By this way, problem is not repeated, customer satisfaction is increased.
4. While classifying problems, category, urgency, impact and priority is defined.
5. Problems can be categorized like hardware, software, supporting software.
6. Problem resolution is monitored according to SLAs.
7. Problem management should monitor the effect of existing problems and known errors on users' services.

General Information:

Table 3-26 General Information about Problem management process

Process ID	P.24
Process	Problem Management
Purpose	Prevent problem and realization of incidents by removing or reducing repeating incidents
Scope	Includes activities required to diagnose the root cause of incidents and to determine the resolution of these problems.
Values to Business	Reduction in the effort to solve incidents over and over again Reduction in the workaround solution cost Increase in availability of IT services and production of IT personnel
Inputs	Incident information forms PSO Security Incidents Details of CI from CMDB in CMS IT Infrastructure Information Authorized Change Plan SLAs
Outputs	RFC Known and accepted errors Problem record Details of Security events and breaches from problem management
Roles	Problem manager Problem solving teams
Tools	Integrated, CMS and KEDB
KPI	The total number of problem recorded in period The number of problems resolved within SLA targets The average cost of handling a problem

Flow Chart:

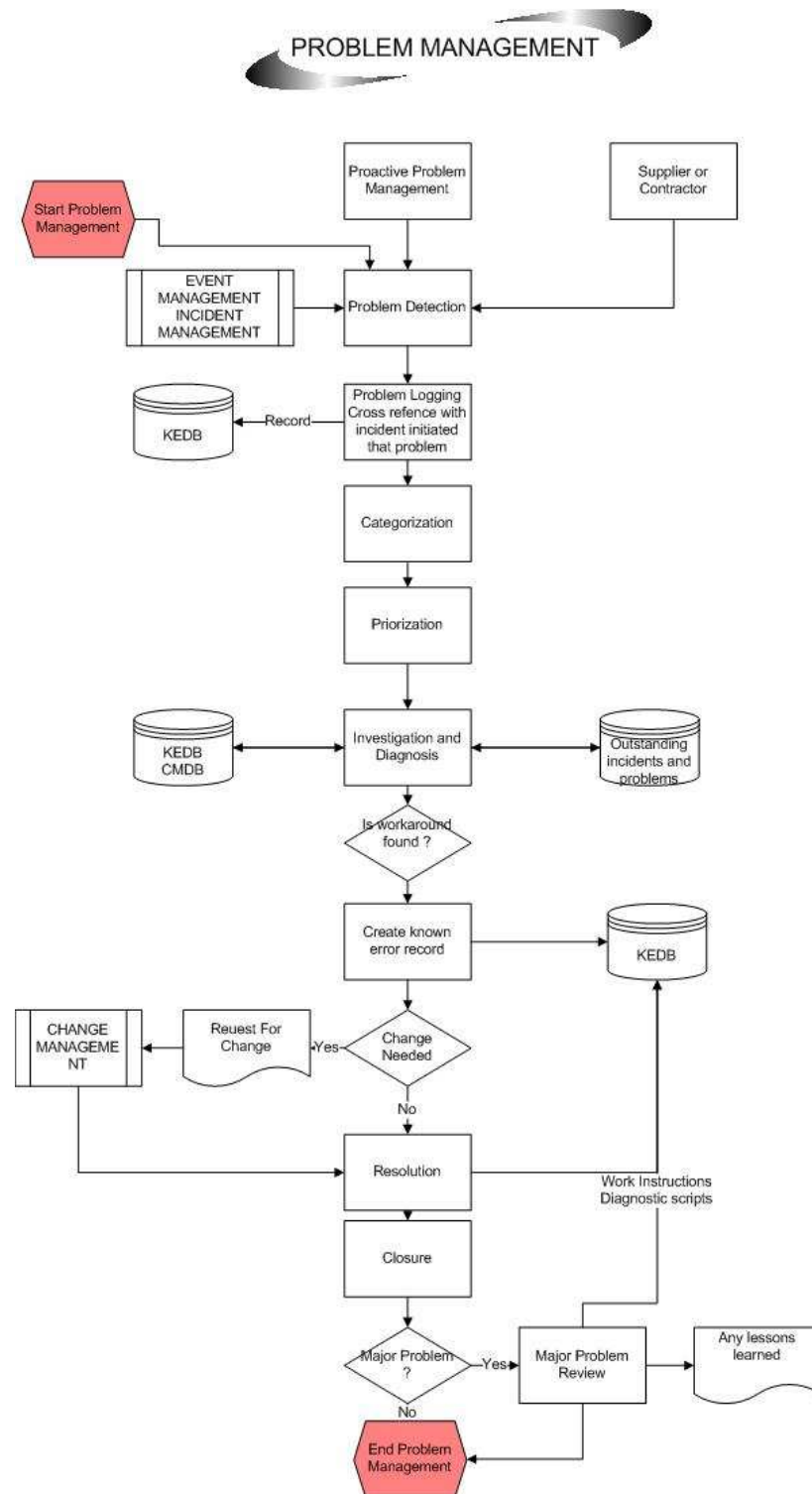


Figure 3-28 Flow chart of Problem management process

P.25 Quality Management

Principles:

1. Standards such as software coding standards, naming guidelines, file formats, chart and data dictionary design standards, users interface standards, standards for development and testing, confirmation standards against requirements, test plans, tests of unit, regression and integration etc. are identified.
2. It should be tried to implement all defined metrics for Service and Service management processes. It should be kept as simple as possible for meeting respective requirements.
3. Framework of service measurement should be determined. Determination of service measurement framework is actually to decide which of the following shall be monitored and measured.
 - ✓ Services, components, service management processes, activities and outputs in processes
4. All roles and responsibilities during service improvement and service quality management should be determined.
5. The most fundamental base is to perform measurement procedure to the extent it is required. Otherwise, once institutions focus on measurement, they experience loss in improving the outcome.
6. Targets of services and service management processes should be SMART. (Specific, measurable, achievable, relevant and timely)
7. Indicators of key performance can be classified in four ways:
 - ✓ Availability: Do you perform?
 - ✓ Quality: Do you perform well?
 - ✓ Performance: How fast or how slowly do you perform?
 - ✓ Value: Does our work create a difference?
8. While designing report, the following question should be responded;
 - ✓ Who is target audience of report?
 - ✓ What shall be report used for?

- ✓ Who is in charge in creating report?
 - ✓ How shall report be created?
 - ✓ In what frequency shall it be created?
 - ✓ Which information shall be created, shared or received?
9. Reports over IT's work contribution should be developed to senior managers. These reports should incorporate realized planning targets, used budget sources, encountered performance targets, and reduced defined risks. It may be expected to receive feedback from senior managers.
 10. Investment profitability is utmost importance for continuous improvement. Previous inconveniences prior to continuous improvement for this process should be calculated no matter how much they might be difficult.
 11. Business Case – Feasibility Case - (Justification for a significant item of expenditure. Includes information about cost, benefits, options, issues, risks and problems.) Business cases should be created.
 12. Business part should be included in quality management in the issue of which improvement shall be effective.
 13. Processes are observed by process owners and preventive or corrective actions are determined.
 14. Following questions should be asked by the Business and IT;
 - ✓ Where are we now? (base level for existing service level)
 - ✓ Where do we want to be? (Work vision, mission, goal and targets)
 - ✓ What do we actually need? (internal and external factors)
 - ✓ How shall we meet? (work budget, IT conditions)
 - ✓ What shall we earn? (IT perception of customer expectations)
 - ✓ What have we acquired? (service presentation and perception)
 15. It should be decided on what and how evaluation shall be performed while making evaluation. There are three potential scope levels;
 - ✓ Only processes
 - ✓ Human, process and technology

- ✓ Full evaluation (Such as acceptance culture in organization, structure and functions of process organization, work IT matching with process environment intermediation)

16. Improvement life cycle is modeled by using Deming cycle (Plan-Do-Check-Act)

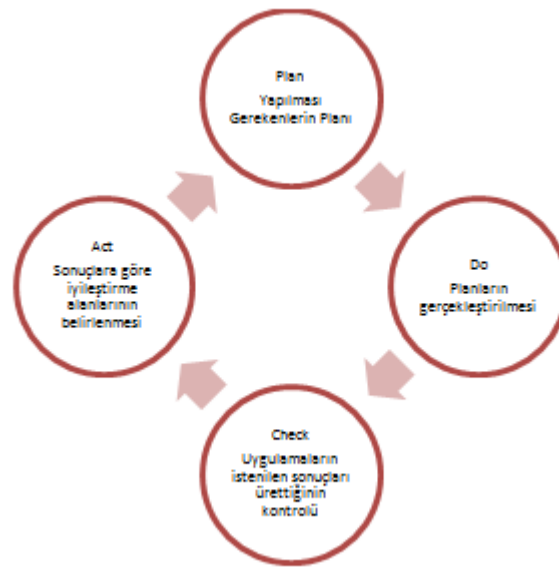


Figure 3-29 Deming cycle

17. One of the most important steps for improvement is benchmarking. (Comparison of his/her organization works in the market with other organizations or the best applications within his/her own body)
18. There are particular procedures to be used for benchmarking; Meeting with customers, personnel or suppliers, in-depth market research, quantitative research, questionnaire, process matching, re-engineering analysis, quality control deviation reports and financial rate analysis)
19. Aforementioned defined improvement process applies identically within benchmarking.
20. There are two types of benchmarking approaches; Internal and External-Third party company) Benchmarking
21. Process maturity evaluation may be calculated according to following CMI maturity model.

Table 3-27 General Information about Maturity Level

0	Non-Existent	Nothing Present
1	Initial	Concrete evidence of development
2	Repeatable	Some process documentation but some errors likely
3	Defined	Standardized and documented
4	Managed	Monitored for compliance
5	Optimized	Processes are considered best practices through improvement

General Information:

Table 3-28 General Information about Quality management process

Process ID	P.25
Process	Quality Management
Purpose	<p>Monitoring performance in conformity with objective in order for providing continuous improvement of IT services</p> <p>Creation of quality management system</p> <p>Monitoring and measuring metrics for continuous improvement of service and service management processes</p> <p>Providing effective and appropriate reporting</p> <p>Defining legal, regulative and contractual conditions and determining compliance level of IT and optimizing in a way which shall reduce risk of non-compliance of IT processes</p> <p>Monitoring internal control processes</p>
Scope	<p>Defining quality standards</p> <p>Measuring internal and external performance according to quality standards</p> <p>Continuously developing quality management system</p> <p>Gathering process performance reports and converting them into management reporting</p> <p>Revising whether it complies with determined objectives and starting up required improvement plans</p> <p>Defining Internal Control system</p> <p>Monitoring and reporting efficiency of internal control</p> <p>Reporting the ones remaining outside of control to management</p> <p>Defining legal, regulative and contractual requirements</p> <p>Evaluating effect of compliance requirements</p> <p>Monitoring and reporting compliance with these requirements</p>
Values to Business	<p>Providing sustainability and quality of presented IT services and making levels of measurement, IT cost, benefit, strategy and service transparent and comprehending these elements</p> <p>Bringing law regarding IT, regulative and contractual conditions compliant</p>

Table 3 -28 (Continued)

Process	Quality Management
Activities	<p>Creation of quality management system (quality requirement and criteria; key IT processes and their interrelation between each other; organizational quality, structure, roles and responsibilities; quality plans are prepared and data created as a result of quality is recorded. Effect of quality management system is measured and developed).</p> <p>Determining particular standards in developing and obtaining service life cycle and sharing this with organization</p> <p>Periodic revision and improvements of quality plan</p> <p>Standard, procedure and implementations should be defined for Key IT processes.</p> <p>Observation approach is determined for monitoring quality of processes and services.</p> <p>Measurable objectives are defined and these measurements are collected. While defining measurable objectives, it should be paid attention that these objectives need to be confirming and measuring business objectives.</p> <p>Observation method such as performance balance scorecard is determined by using these data. Observation is performed via this method and outcomes are recorded. These technical performance evaluations need to be converted into management reports.</p> <p>Progressive and improvement actions are defined and implemented for improvement of evaluated performance.</p> <p>This information is evaluated by process owners and corrective and preventive actions are included.</p> <p>“Environment” and control framework of IT Control are continuously observed and it is evaluated and developed comparatively.</p> <p>Monitoring and evaluation of efficiency of IT executive audit controls</p> <p>Determining extraordinary cases in control, making justification and reporting these exceptional cases to stakeholders</p> <p>Evaluation of completeness and efficiency of control over IT processes, policies and agreements of management</p> <p>If required, ensuring completeness and efficiency of internal controls by third parties</p> <p>Evaluation of internal control case of external service providers and confirming compliance of external service providers to obligations arising out of contract as well as legal and regulative conditions</p> <p>Complete efficiency evaluation of manager assessment over IT processes, policies and contracts</p> <p>Defining, starting-up, monitoring and implementing improvement actions arising out of control evaluations and reporting procedures</p>

Table 3-28 (Continued)

Process	Quality Management
Activities (Continued)	<p>Definition of compliance terms of local and international guidelines, external legal and regulative legislation and contract</p> <p>Revision, regulation and confirmation in a way which shall be in conformity with IT policies, standards, procedures and methods, external legal, regulative and contract conditions</p> <p>Compliance reporting; If there is lacking in compliance, making sure that corrective action has been applied on time process owner</p> <p>Integration of IT Reporting of Legislation, legal and contractual requirements with similar outputs of business functions</p>
Inputs	<p>Reporting performance of all processes</p> <p>SIP and Service Quality Plan</p> <p>Reporting Project Performance / Project Plan</p> <p>Reports of Customer Satisfaction (Service management, service desk)</p> <p>Reports of monitoring after Change (Change Management)</p> <p>Cost-Benefit Reports (Financial Management)</p> <p>Service Performance Information and reports</p> <p>Details of Security events and breaches from incident management</p> <p>Risk Reporting</p> <p>Metrics for evaluating application performance</p> <p>Review action parameters (input for CSI)</p> <p>Security Audits and audit reports</p> <p>Supplier and Contract Performance information and reports and Supplier Service Improvement Plan</p> <p>Improvement ideas for Continual Service Improvement</p> <p>IT Policies</p>
Outputs	<p>Improvement actions plans</p> <p>History risk tendencies and events</p> <p>Reports regarding efficiency of IT Controls</p> <p>Catalogue of efficiency of IT controls</p> <p>Catalogue of legal and legislative requirements</p> <p>Compliance reports of IT activities with external legal and legislative requirements</p> <p>Development Standards</p>
Roles	<p>Quality Manager</p> <p>Service Manager</p> <p>CSI manager</p> <p>Service/process owner</p> <p>Reporting analyst</p> <p>Service Knowledge management process owner</p>

Table 3-28 (Continued)

Process	Quality Management
Tools	Integrated Change Management, CMS and KEDB (Known errors database)
KPI	Rate of errors released prior to productions Reduction rate in the number of high critical incidents at the beginning of month per user Rate of IT project meeting quality objectives signed and monitored by quality assurance Rate of IT processes meeting quality objectives and monitored regularly by quality assurance Amount of stakeholders satisfied with measurement process Rate of monitored critical processes Number of performance objectives met Number of rehabilitation actions arising out of measurement activities Frequency of internal control incidents Number of control rehabilitation initiatives Number of legislation and legal non-compliance cases Number of on-time actions over internal control problems Number of yearly-based critical non-compliance problems Frequency of revising compliance of legislations

Flow Chart:

Activities of Quality management process cannot shown as flow chart. There exist a flow chart only for improvement services activities.

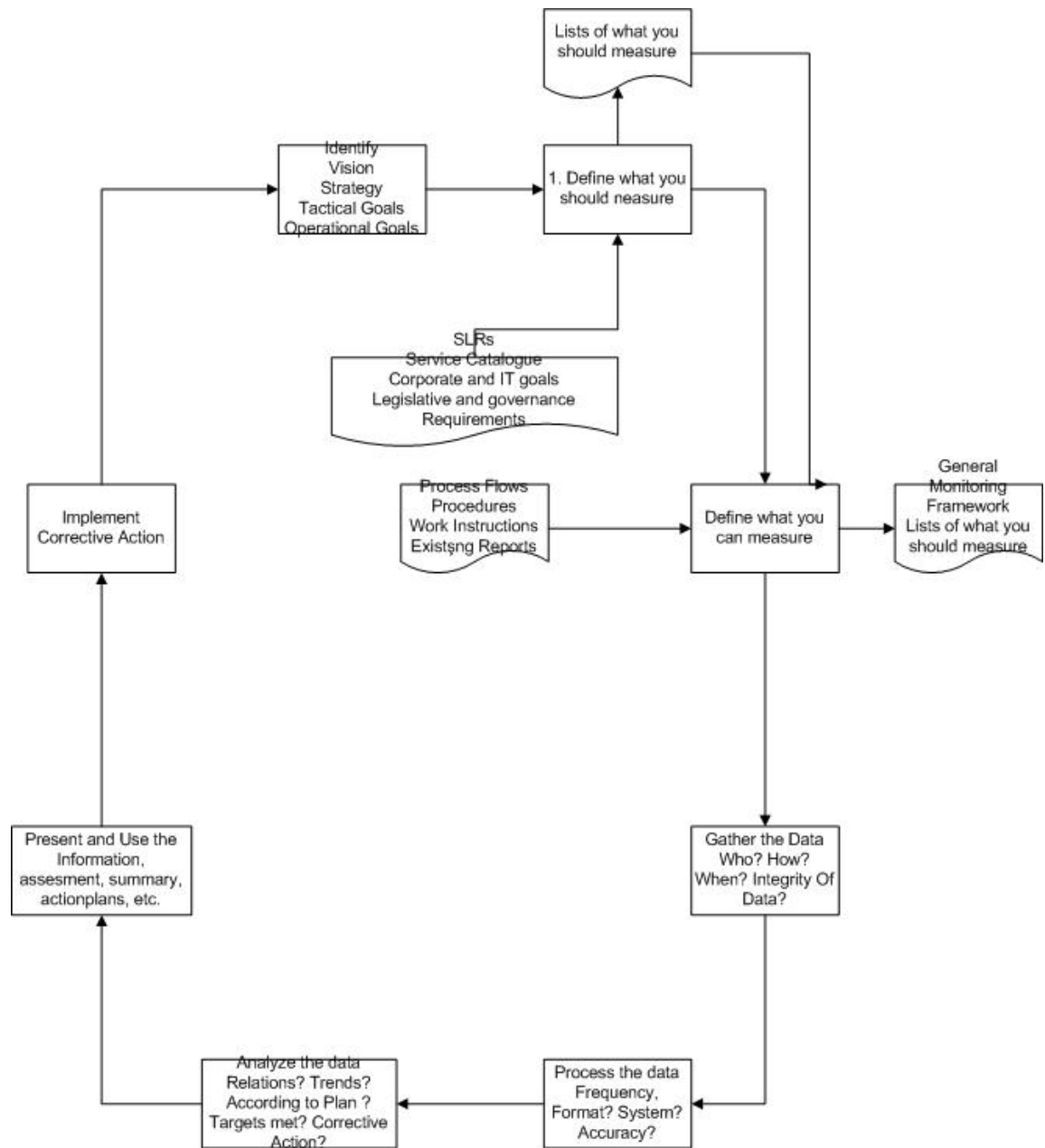


Figure 3-30 Activities while improving services

3.2.3 Functions

F.1 Service Desk

It is a functional unit consisting of personnel in charge with different service through infrastructure events reported automatically, service desk, telephone or Internet. Service desk is only point contacted with IT users, namely, it is only connection point. (Single Point of Contact) (SPOC) Thus, since this is an opening door of IT to user, this is quite important entity.

Purposes of Service Desk

Primary purpose is to rapidly solve the problem received from customer as soon as possible or to evaluate the request received from customer. Thus, customer satisfaction is boosted. There are other responsibilities apart from these elements listed;

- ✓ Recording detailed information of request and problems received from user
- ✓ Recording the events received as an incident from Event Management
- ✓ Conducting research and attempting to solve problem
- ✓ Solving requests and problems received
- ✓ Access rights received for simple systems are performed if they have authority
- ✓ Escalating the problems not solved or the request not performed to upper stage within contemplated period
- ✓ Informing users about the problem and request which has been constantly notified
- ✓ Closing performed requests or solved problems
- ✓ Conducting questionnaire for measuring user satisfaction
- ✓ Informing user periodically about in what stage received problem is
- ✓ Conducting tendency analysis regarding incidents

Structure of Service Desks

There are several methods for configuring service desk. These methods are:

- ✓ Local Service Desk: It is found in the same or physically nearby places with supported users.
- ✓ Central Service Desk: It is installation of service desk in one point. In this way, number of service desk is reduced.
- ✓ Virtual Service Desk: It is possible to create impression of central service desk via such type of service desk by using specifically Internet and supporting tools with the help of technology no matter how much users are in different places and in geographically different locations.
- ✓ Service Desk Following Sun: Two or more service desks are situated in different continents for rendering 7/24 service and they are integrated accordingly.
- ✓ Specialized Service Desk Groups: Incidents regarding particular IT service may be directly oriented to specialist group.

Service Desk Performance Measurement

Some criteria should be created for measuring performance of service desk. Examples to this occasion are as follows:

- ✓ Rate of solving the problem and the request received from service desk
- ✓ Average time of incidents solved through service desk
- ✓ Average time elapsed until delivery of incidents not solved through service desk to upper stage.

Service Desk Roles and Responsibilities

- Service Desk Manager
- Service Desk Supervisor
- Service desk analyst
- Super users

Supervisor/Manager of Service Desk:

- ✓ Managing all desk activities and supervisors

- ✓ Notifying big cases affecting the work to senior managers
- ✓ Participating to meetings of change consultancy board
- ✓ Performing escalation of the problems and the requests not having been solved
- ✓ Creating statistical and management reports via service desk logs
- ✓ Informing service desk analysts regarding performed changes, if any
- ✓ Acting together with top executives and Change management

Super Users:

- ✓ Provides communication between IT and work on operational level
- ✓ Supporting expectations of users
- ✓ Providing training of personnel in their own areas
- ✓ Providing support to service desk in minor lines or requests

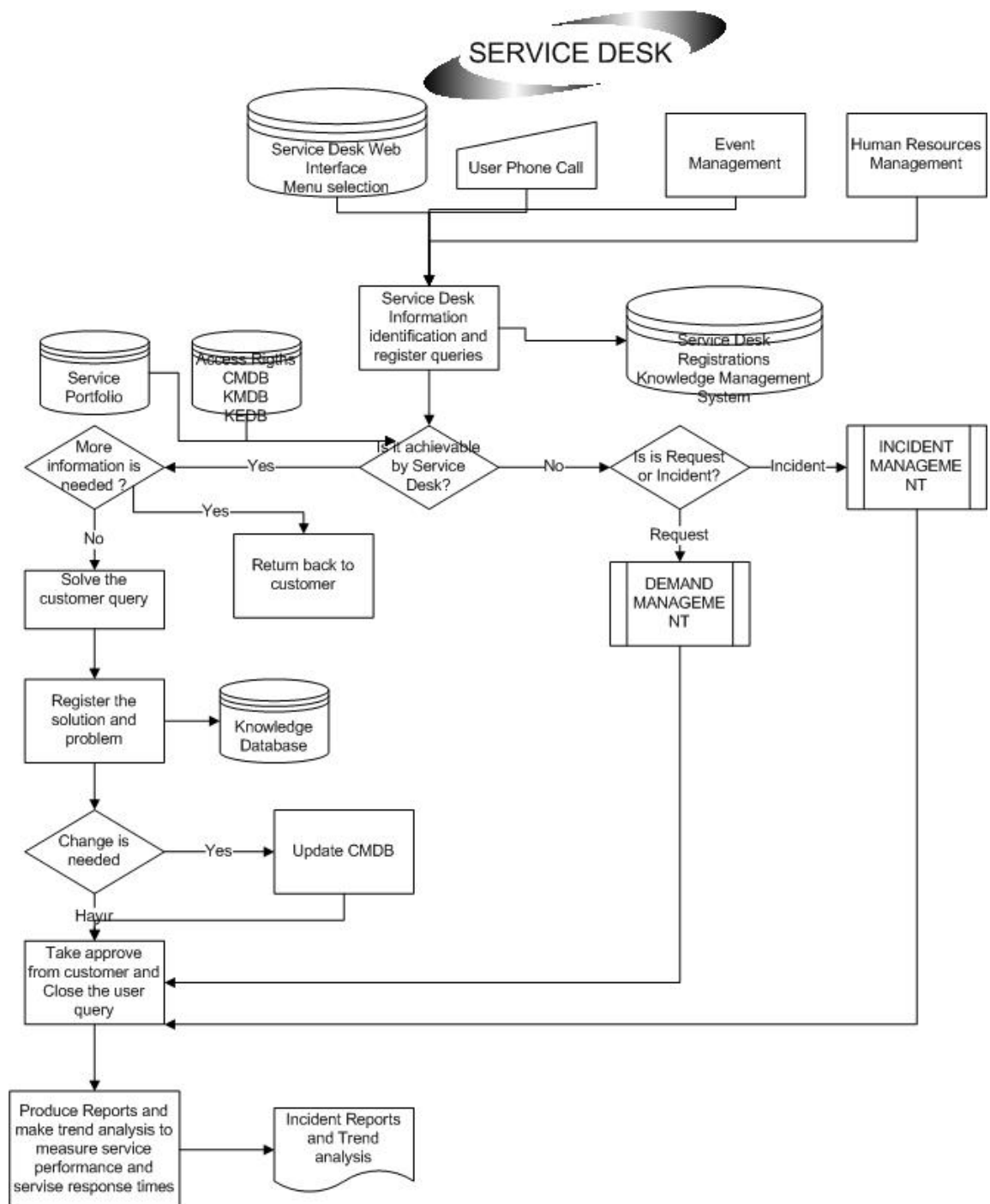


Figure 3-31 Flow chart of Service Desk

F.2 Application Management

1. Application management manages application during life cycle. This group plays a major role in designing, testing and developing of applications comprising parts of IT services.
2. Purpose: It supports business process by determining functional and managerial needs of application software. Afterwards, it assists continuous support and development and design and loading of these applications.
3. Study of whether needs shall be met or not shall be performed. (Feasibility)
4. It determines alternative application actions likely to meet the needs and presents this to business section. Benefit of these solutions towards IT operational and business is evaluated.
5. Alternatives along with business part are evaluated and approved.
6. It decides on purchasing of applications or in-house development.
7. As an output, Business requirement feasibility is included.
8. If application decides on purchasing procedure, procedure of configuration of taken application is performed according to business needs. At the same time, Application Management makes preparations to SLA along with customer by looking into respective needs. Several documents are formed by Application Management Groups. List of these documents in summary is as follows:
 - ✓ Application Portfolio: It is a part of Service Portfolio. It should incorporate key features such as customer and users of application relating to application, work purpose, architecture, developers of application, support groups etc. Application needs have four different types: Functional needs, Managerial Needs, Usability needs and test needs.
 - ✓ Use and Change Cases: It documents use of application along with real life scenarios for demonstrating limits and functionality of application. Change cases are act of estimation of potential change effects likely to occur towards application function, architecture or utilization by using scenarios.

- ✓ Manuals: Three documents are created as being Design Manual, Management Manual and User's Manual. Though these documents, in fact, are created by application developers, Application Management checks compliance of these documents.

Activities of Application Management:

1. Determining functional and technical requirements of business and performing their maintenance
2. Analyzing applicability of these requirements
3. Presenting alternative ways for fulfilling these requirements
4. Obtaining approval of above first, second and third items

All activities which have been performed for Technical Management Infrastructure alongside with aforementioned four articles are required in order for applications to be performed by Application Management.

Specific metrics may be created for measuring this function. These are:

- ✓ Rate of stakeholders who are satisfied with accuracy of feasibility study
- ✓ Rate of realization of feasibility study on time and with determined budget.

Roles;

- ✓ Applications Managers/Team leaders
- ✓ Applications Analyst/Architect

F.3 Technical Management

1. Since Technical Management groups have technical information in respect with IT Infrastructure management in organization, they play an influential role in this

regard. This group supports these processes by providing resources to IT service management processes.

2. Technical management groups are responsible for operating several service management processes and creating documents in regard with IT infrastructure and maintain such documentations. They are liable for creating and maintaining documents relating to several processes such as capacity plan, change management, problem management. These documents are;
 - ✓ Creation of Technical Manual
 - ✓ Management and administration manual
 - ✓ User manual for configuration personnel
 - ✓ Creation and sustainability of technological infrastructure
3. Technological Management makes preparation for operational level agreements (OLC) along with customers by looking into the requirements at the same time. Primary goal of Technical Management;
 - ✓ Preparing plan for procurements relating to technological infrastructure
 - ✓ Ensuring protection and existence of infrastructure sources
 - ✓ Maintenance of infrastructure
 - ✓ Well-designed, flexible and cost-effective technical topology
 - ✓ Utilization of sufficient technical information for performing maintenance of technical infrastructure maintenance in optimum condition.
 - ✓ In case of technical problems, solving this problem rapidly by using technical information
 - ✓ Implementing internal control, security and auditing

Activities of Technical Management

1. Defining information and experience required for management and operation of IT Infrastructure
2. Developing skill inventories and performing training requirement analysis

3. Performing training requirements of users, personnel of service desk and other groups
4. Incorporating IT services in architecture of technical infrastructure and performance standards
5. Performing IT Infrastructure management activities within the scope of Technical Management
6. Performing outsourcing supply phase of configuration personnel
7. Defining tools and standards required for case management
8. Creating second line support for escalation realized on service desk in incident management
9. Being include in coding system required for classification of technical management and problem
10. Providing technical information required for evaluating changes in change management
11. Defining improvements required for technological infrastructure
12. Performing supply, implementation and maintenance of technological infrastructure meeting business functional and technical requirements
13. Utilization responsibility of property infrastructure elements should be defined and their utilization processes should be monitored and evaluated
14. Changes in respect with infrastructure should be handled with the process of Change Management
15. Development and test environments should be installed for feasibility and integration tests of infrastructure components
16. Preventive Maintenance for Hardware: It is the operation of procedure preparation and implementation of this procedure for infrastructure maintenance

Technical Groups consists of following teams:

- ✓ Server Management and Support (Performs procedures relating to server. Performs procedures such as maintenance of operating system in which server is

running, security of servers, definition and management of virtual servers, capacity and performance of servers, removal or disposal of old server).

- ✓ Network Management (Responsible for LAN, MAN and WAN and Network providers of institution)
- ✓ Database Management (Needs to co-operate with software life cycle)
Creation of database standards, design and test of database, third level support in lines relating to database, backup of database, determining archiving and storing strategy, measurement of database performance, etc.
- ✓ Directorate Servicer Management
- ✓ Desktop Support
- ✓ Middleware Management
- ✓ Internet /web management
- ✓ Storage and Archive

Roles;

- ✓ Technical managers/team leaders
- ✓ Technical analyst/architects
- ✓ Technical Operator

F.4 Operational Management

1. IT Operation management groups consist of personnel of technical management and application management group.
2. This group performs daily activities required for study of IT infrastructure. It has two tasks:

Operation Control:

- ✓ Console Management: It incorporates daily monitoring and controlling activities.
- ✓ Job Scheduling: It performs standard routine works, queries or reports which technical and application management teams of IT operations has delivered

accordingly. Performing programming by listing works, processes and tasks efficiently for making use of them in this regard as well as maximum efficiency of business requirements.

- ✓ Backup and Restore: Procedure of backing up data whose backup shall be received determined within the scope of recovery plans and performing recovery procedures if necessary is performed in continuity management. Data received is determined where they shall be stored. Remote locations to be protected in terms of security shall be, too, stored. Backup strategy should be determined. Content of this strategy entails where received backups shall be stored, how much time they shall be preserved, in what forms they shall be kept and who shall access such data.
- ✓ Restore: Restore procedure may be required due to information requirement required to be searched from old data or from discarded data, lost data and disaster recovery plan.
- ✓ Print and Output: Information is generally in electronic environment (printouts) or they are printed. Obtaining critical data should be provided in a way which shall be physically safe in law and regulations. For instance, printers with special purpose, special forms, security symbols or valuable document.

Manage the Physical Environment

- ✓ It shall provide appropriate physical environment for protecting from access to IT assets, damage and theft and its current should be maintained.
- ✓ Selecting location for IT Equipment and risks likely to occur while performing design of location arrangement should be taken into consideration.
- ✓ Physical security measures in the same line with work requirements for location and physical assets should be defined and applied.
- ✓ Physical security measures risks are performed with effective prevention, recognition and reduction procedures. These risks are:
 - Stealing, temperature, fog, water, fire, terror, quake, destruction, power cut, chemical substances and explosives.

- ✓ It is required to define and implement a procedure for handling emergency cases and accessing these locations. It is required to confirm, authorize, log and monitor accessing procedures to such areas. This monitoring procedure should be valid for all people.
- ✓ Measures should be taken for being protected against environmental factors. Some special devices should be placed to environment in order for monitoring and keeping under control.
- ✓ It is essential to manage physical facility along with laws and regulations, technical and business requirements, supplier specifications and health and security manuals.

IT Operation Management Groups are responsible for creating following documents and maintaining these documents accordingly.

- ✓ Standard operating procedures: Containing detailed instructions and activity schedules for every IT Operations management team. These documents cover routine works.
- ✓ Operations Logs: Any activity of IT operation is recorded.
- ✓ Shift Schedules: It is an act of documenting activities to be performed during changing of Shift Schedules in a form of draft.
- ✓ Operations Schedule: It is similar to Shift Schedule but it covers all IT operation. It is included within operations schedule along with all planned changes, maintenance, routine works and additional works as well as information of newly-received works.

Roles;

- ✓ IT Operations manager
- ✓ Shift leaders
- ✓ IT Operations analyst
- ✓ IT Operators

CHAPTER 4

WEB BASED APPLICATION: IT Processes Guide

In this chapter, firstly general information about the IT Processes Guide (ITPG) will be explained detail, after that, design of it is given and lastly in the third section, imaginary case for ITPG is shown.

4.1 General Description

ITPG provides a web based application to two different user types which are beneficiary and occupier. Users can reach processes that meet the COBIT and ITIL requirements completely and start to adapt to CMMI and Information Security Management System which should be implemented by the organization to govern IT effectively and efficiently. Also for beneficiary user types, ITPG provides organizations to define their own processes in a web based application to make easy of the reach to the information about processes and manage them.

ITPG is a web-based application developed using Visual Studio 2008 as an application platform, MS SQL Server 2005 as a Database management system and Visual Basic as a programming language. It is developed to run on Microsoft environment with .Net Framework Version 3.5, IIS V 6.0. Main components of ITPG are the Knowledge Bank containing static web pages and Organization IT Processes Management containing dynamic web pages.

User operations (adding new user, deleting new user or updating user authorities) are managed by the administrator of ITPG.

4.1.1 Constraints, Assumptions and Dependencies

- Since program is prepared by using Visual Studio 2008, it works only Microsoft based operating systems.
- Because of the language of web site, it is only used by people who understand Turkish.
- The usage of site is process based and only the attributes of processes which are defined before can be operated by the occupier.

4.2 Design of IT Processes Guide

In the following subsections, firstly database design of the ITPG will be explained; the second subsection provides information about design of software of ITPG.

4.2.1 ITPG Database Design

ITPG is prepared by using SQL Server 2005 as a database. ITPG has one database named as “ITPG”. Tables in figure in ITPG have been composed by thinking dynamic web pages in Organization IT process management component of ITPG.

Main Tables in Organization IT Process Management

ER Diagram of the following tables is given in Appendix B.

Table 4-1 Tables in ITPG database

TABLE NAME	TABLE EXPLANATIONS
TB_USER_INFO	Holds the information about users
TB_ORG	Holds the information about the organization of each user
TB_ORG_PRC	Holds the information about all processes of the corporation
TB_ORG_HEDEF	Holds the information about purposes of all processes of the corporation
TB_ORG_INPUT	Holds the information about input of the all processes of the corporation
TB_ORG_OUTPUT	Holds the information about output of all processes of the corporation
TB_ORG_KAPSAM	Holds the information about scope of all processes of the corporation
TB_ORG_METRIK	Holds the information about KPI (Key Performance Indicators) of all processes of the corporation
TB_ORG_RESIM	Holds the information about flow chart graphic of all processes of the corporation
TB_ORG_ROL	Holds the information about roles of processes of the corporation
TB_ORG_RESPON	Holds the information about responsibilities of all roles defined before of the corporation
TB_ORG_DEGER	Holds the information about processes' value to business of the corporation
TB_ORG_TANIM	Holds the information about all processes definition of the corporation
TB_ORG_ESAS	Holds the information about all processes principles of the corporation

4.2.2 ITPG Software Design

In this chapter, software design of the ITPG is explained. Design is covered by two modules of the ITPG; Knowledge Bank and Corporate IT Process Management which are explained in the following chapters in detail.

To explain each operation for each module, use case diagrams by using “Visio 2007 UML Use Case” and activity diagrams by using “Visio 2007 UML Activity” are provided.



Figure 4-1 ITP Guide Modules

Use Case diagram for ITPG are given in Figure 4-2;

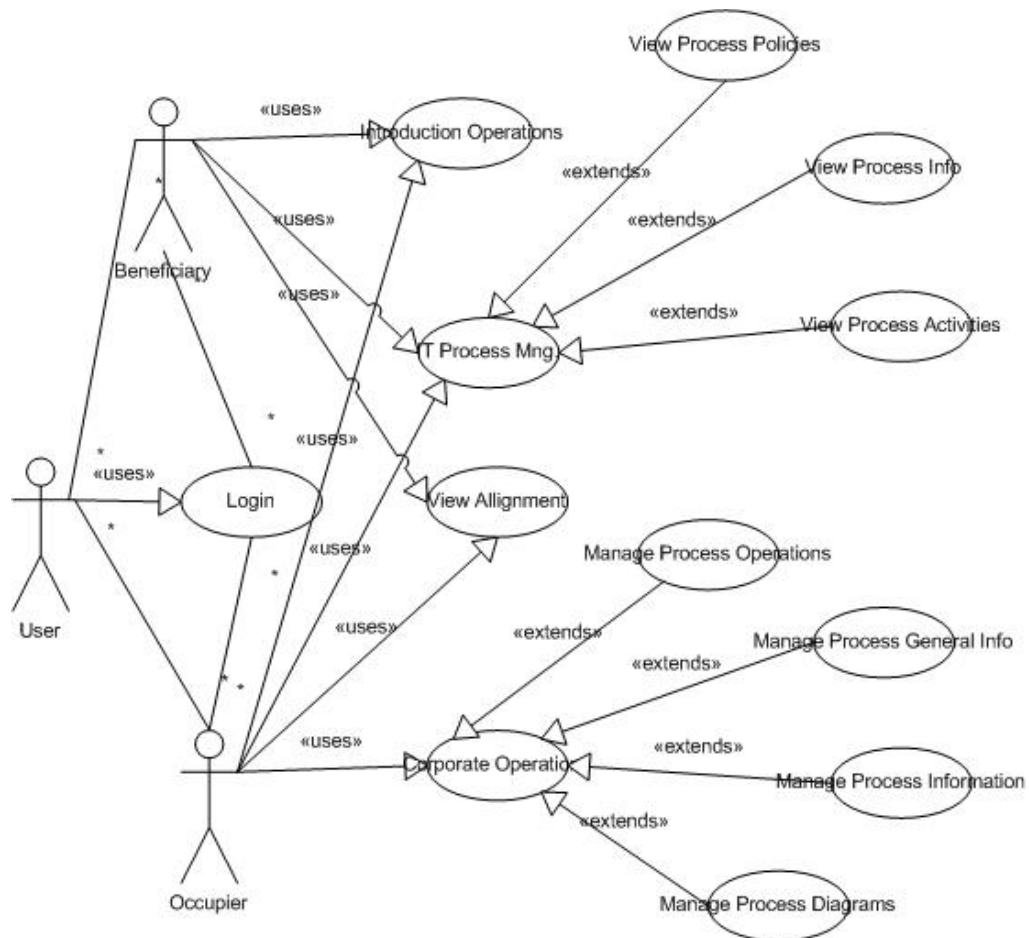


Figure 4-2 Use case diagram of ITPG

IT Processes Guide

As seen in use case diagram, there exist two types of user; beneficiary and occupier. There are 12 use cases which are Login, Introduction Operations, IT Processes

Management, View Process Policies, View Process Information, View Process Activities, View Alignment, Corporate Operations, Manage Process Operations, Manage Process General Information, Manage Process Information, Manage Process Diagrams used for describing the system. Extends and uses of each use cases are given in Use case diagram. All cases are explained in detail by the help of activity diagrams.

4.2.2.1 Login

User enters the application through Login page. User enters username and passwords into the application. Authentication level is determined through login action and related functionalities are determined.

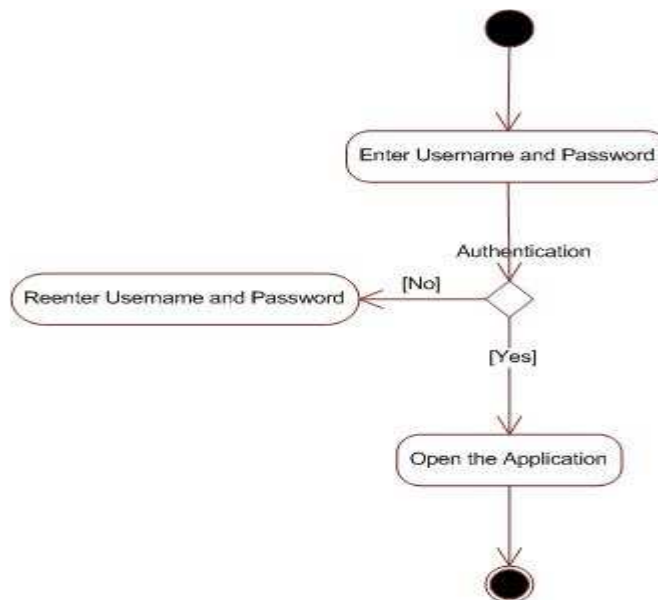


Figure 4-3 Login activity diagram

4.2.2.2 Introduction Operations

All user type can reach these operations. Definition of Basic concepts, which are IT service management, IT Governance, Process Management, definition of based

standards in the scope of web site, frequently asked questions and intellectual property rights can be reached through this use case.

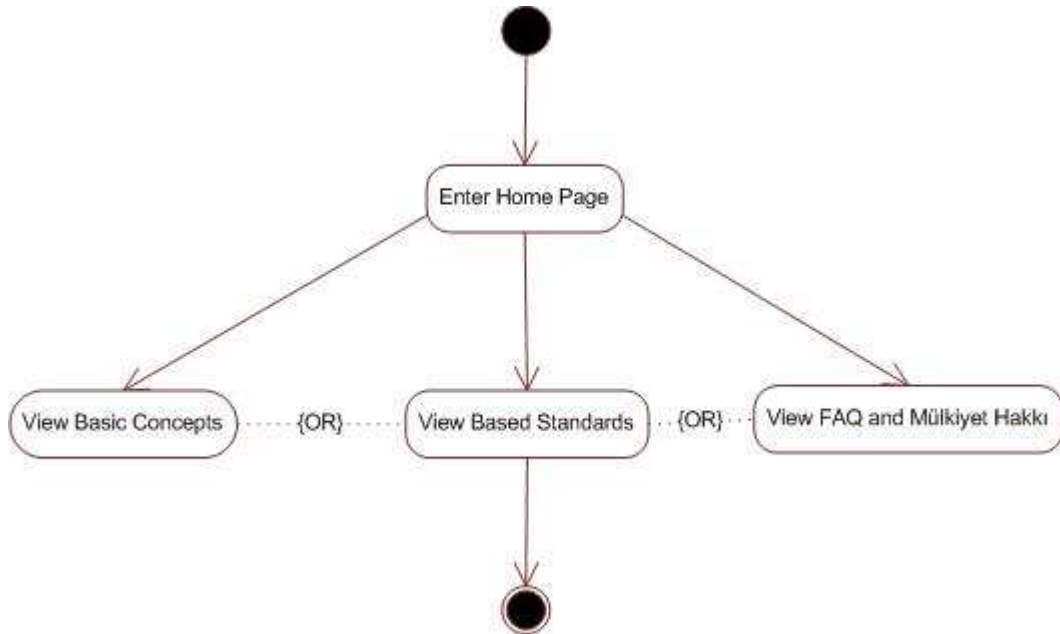


Figure 4-4 Introduction operations activity diagram

4.2.2.3 IT Guide Processes

All user type can reach this use case. In this use case, users can view the scope of IT process management, IT service management processes and functions, role term, tools selection and dictionary.

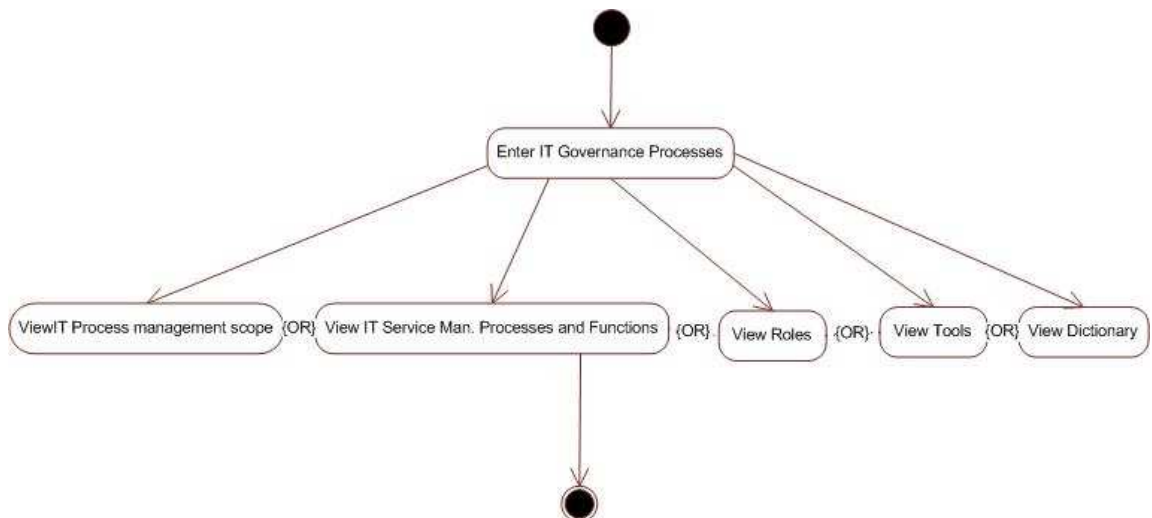


Figure 4-5 IT Processes Guide Activity Diagram

4.2.2.4 View Process Policies

In this use case, principles of these processes are viewed.

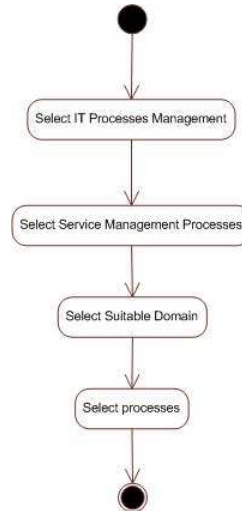


Figure 4-6 View process policies activity diagram

4.2.2.5 View Process Information

By using this use case, attributes of these processes which are definition, goal, scope, value to business, roles, input, output and metrics are viewed.

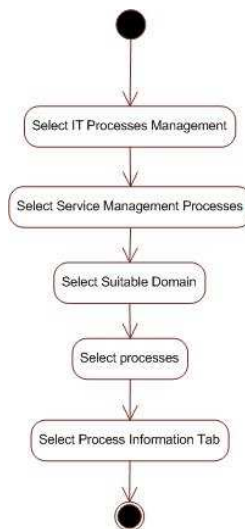


Figure 4-7 View process information activity diagram

4.2.2.6 View Process Activities

From this use case, if the activities of process can be visualized by using flow chart then flow of the process is shown. Otherwise activities are written in text format. There is also a link to bigger the figure of the process flow.

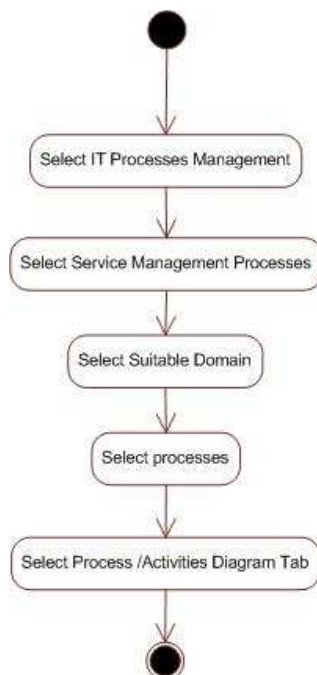


Figure 4-8 View process activities activity diagram

4.2.2.7 View Alignment

In this use case, user can reach the alignment of the defined processes with the ITIL and COBIT which is wide spread in the world. (Callahan, 2004) User can view the Processes –ITIL; ITIL – Processes; COBIT – Processes; Processes – COBIT.

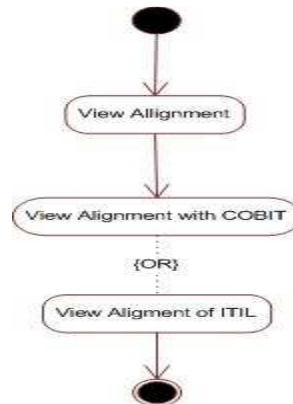


Figure 4-9 View Alignment activity diagram

4.2.2.8 Corporate Operations

For each organization which has authority to use this application of which user type is occupier, there exist some operations to manage their IT processes such as create new processes, their attributes and adding process flow chart.

4.2.2.9 Manage Process Operations

This use case provides organization to define their own processes in a web based application to make easy to manage their processes and deliver their processes through their organization easily. Occupier can create new process, delete or update existing processes totally. When an existing process is deleted, all attributes and process flow chart, if it exists, are also completely deleted. While entering process name, there is no constraint.

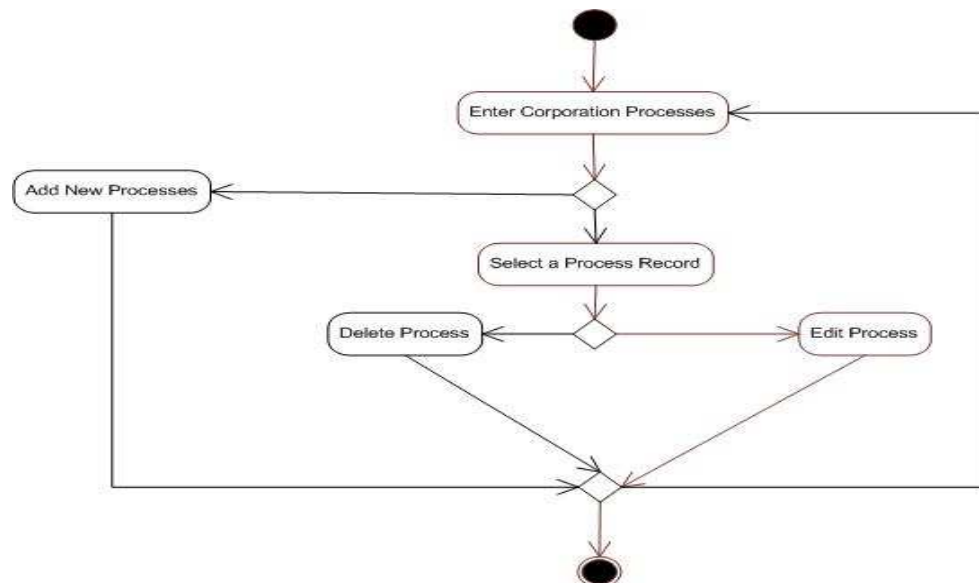


Figure 4-10 Manage process information activity diagram

4.2.2.10 Manage Process General Information

In this use case, occupier, can create, delete or update processes general attributes; definition, goal, scope, value to business and principles one by one. There is no maximum number limit for user to add each attribute.

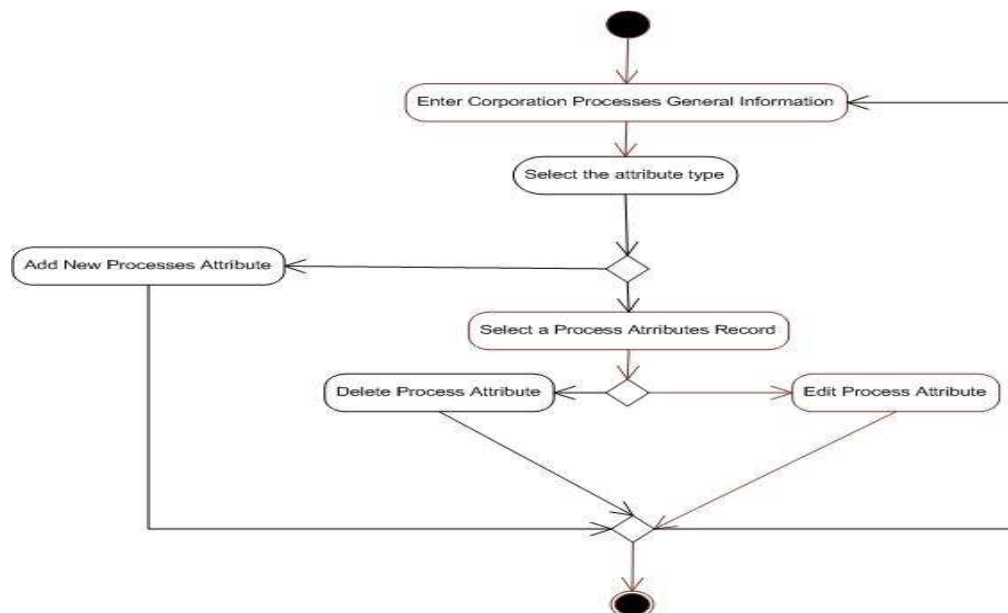


Figure 4-11 Manage process general information activity diagram

4.2.2.11 Manage Process Information

In this use case, user, occupier, can create, delete or update processes attributes; roles, responsibility for each role, input, output and metrics one by one. There is no maximum number limit for user to add each attribute.

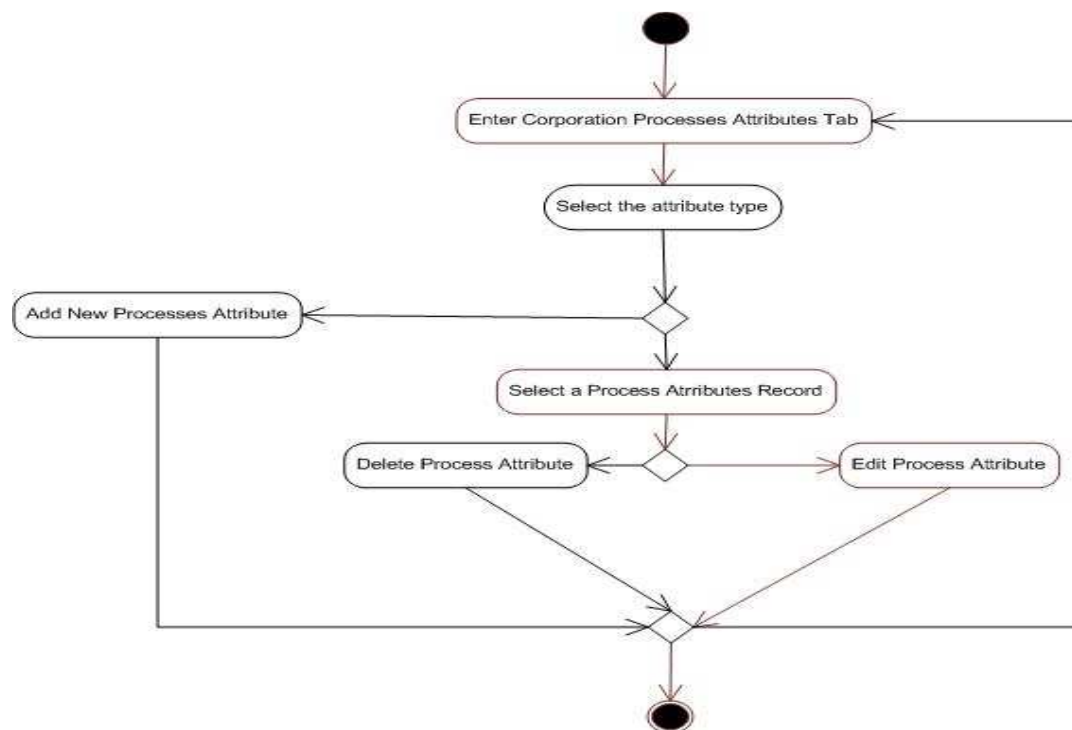


Figure 4-12 Manage process information activity diagram

4.2.2.12 Manage Process Diagrams

User can remove or view in a bigger format if there exists a before added process flow chart or add process flow chart only if there is no added diagram before. User can add diagram in a “pdf”, “jpg”, “doc”, “docx”, “xls”, “xlsx”. User can add maximum 250 kb size. If the process flow chart cannot be seen clearly, user can click the link to see figure bigger.

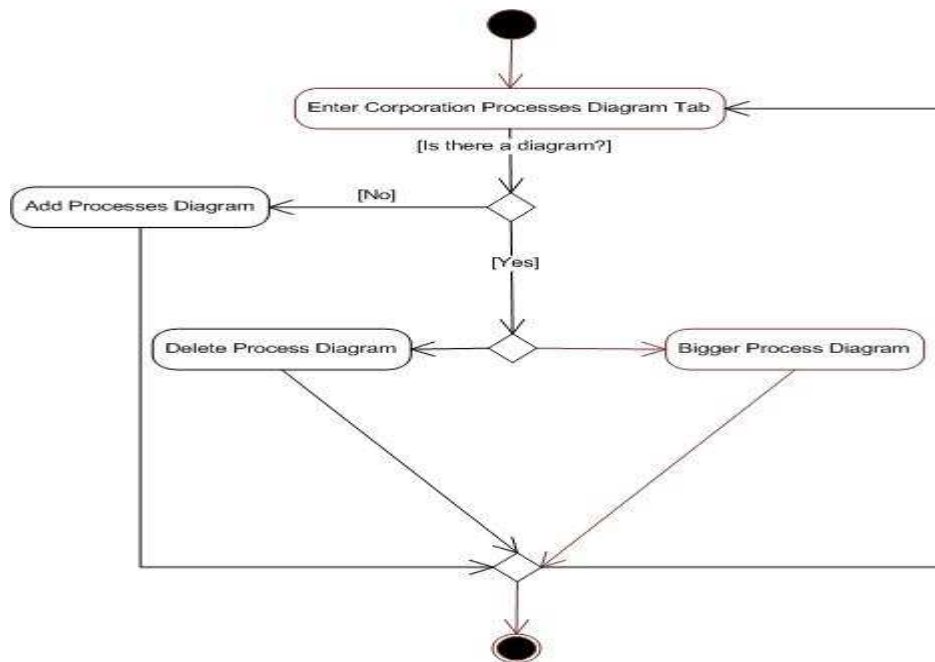


Figure 4-13 Manage process diagrams activity diagram

4.3 An Imaginary Case Study for of IT Processes Guide

Although this tool is ready for use, it has not been tested for organization because it has not been commercialized yet. Implementing all processes in an organization which gives an opportunity to justify defined processes formed in the scope of thesis takes at least 6 months so no time to use this tool. And also, the organization which processes are implemented can have their own tool to manage processes, there is no need to use. On account of the reasons mentioned above, IT Processes Guide (ITPG) is not justified yet. But an imaginary case study is done to justify ITPG partially.

The application is set up on a server in Informatics Institute. It is ready for use. The web address of the application is <http://144.122.98.49/ITGovernanceProcess/MainPage.aspx> Since knowledge bank operations do not have dynamic pages, they are not explained in this part.

Corporate IT process management operations are shown in detail with interfaces by providing an imaginary case.

ITPG is used as a tool to manage their IT processes by an imaginary BA university. BA University provides IT services to students, assistants, employees and instructors of university. BA University provides the following services; arranging and managing courses taken by students and given by instructors, organizing content of each course, MS/PHD application, online exam taking. In addition to these, it also provides information to students about each department information, academic rules and regulations, mail and forum services.

Assumptions and Constraints for Organization BA;

1. BA University has an internal IT.
2. The IT organization is composed of three departments which are Software team, executive managers and system management team.

Firstly, before starting to use the tool, organization has to define their vision, mission and strategy. First and foremost, organization makes sure and believes that it needs their processes in the organization and services delivered have to be managed. Otherwise, failure is unavoidable.

Before defining which processes organization should start, organization can review introduction to service management guideline defined in IT Processes Guide web application.

Then, company can define their processes. It is given in Figure. As an example, organization defines their Configuration Management Process.



Figure 4-14 An example of page that defining process

After adding the process name, company can automatically directed to Processes attributes page to define the attributes of processes. This page contains three tab; Process General Information, Process Information and Process Diagram. User can start with any tab to add attributes. In this case, it is started by adding attributes which are in Process General Information.

In process general information, there exists five attributes (Definition, Goal, Scope, Value to business and principles) that can be added as stated above. Each attributes should be added separately i.e. when any information can be added for any attribute, then “ADD” button below the attribute should be clicked to finish the operation. Company gives the definition of the process by using this page. It is shown in Figure 4-15.

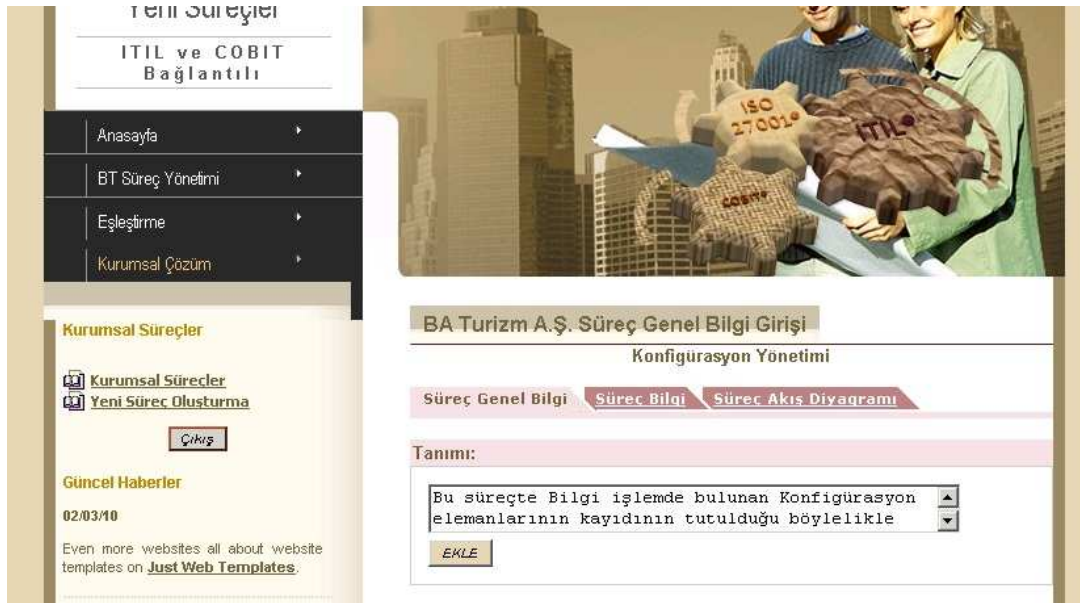


Figure 4-15 An example of page that defining definition of process

The other attributes in Process General Information can be added similarly.

In the next step, company defines Process information attributes (roles, responsibilities for each role, input, output and metric) by clicking Process information tab. Similar to Process general information, roles, responsibilities, inputs, outputs and metrics of the process are added one by one. To figure out that operation, organization adds roles of process.

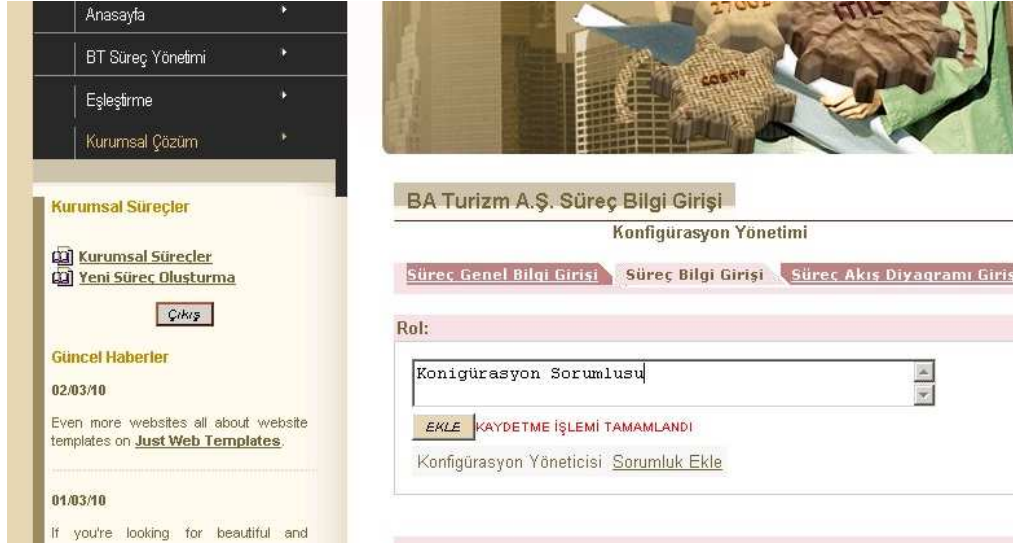


Figure 4-16 An example of page that defining role of process

After adding role of the process, by selecting this role company defines responsibility of the role. This representation is given in the following figure.



Figure 4-17 An example of page defines responsibility of selected role of process

The other attributes of Process Information can be added similarly. In the fourth step, company inserts the process flow chart if any.



Figure 4-18 An example of page that uploading flow chart of process

Company view all existing processes defined before by clicking Company Processes. In this page, company deletes or updates processes viewed.

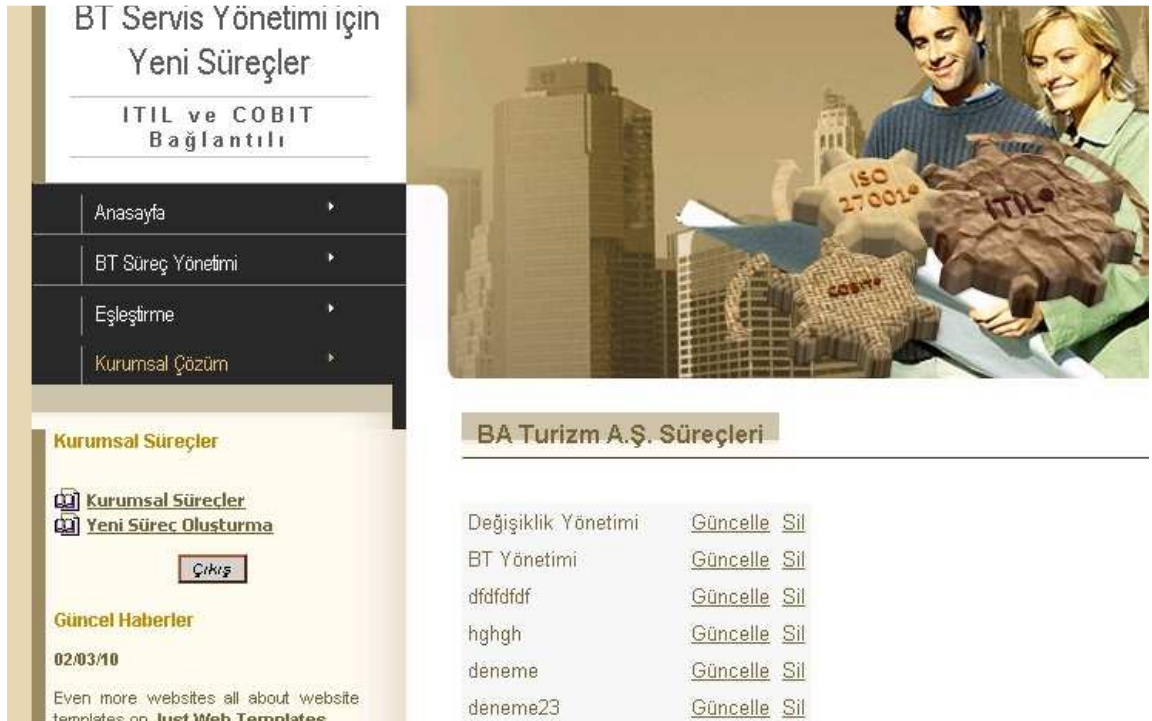


Figure 4-19 An example of page that showing existing processes

Company updates and deletes all attributes of defined process. As an exemplary, company updates responsibility of the role defined in Configuration Management process. Company selects the process of which attributes are planned to be updated and select the “Show Responsibility” of the row of role that want to be updated.

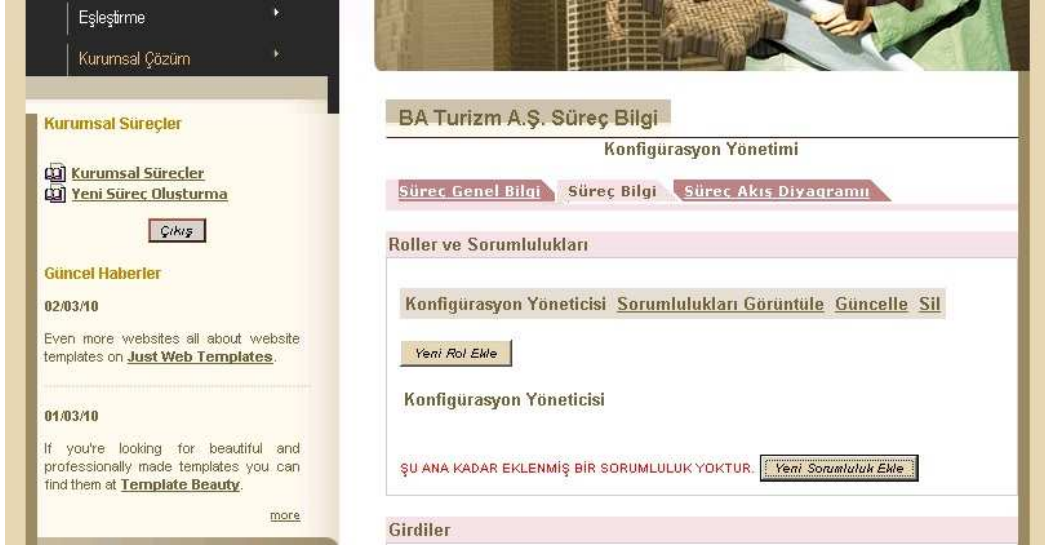


Figure 4-20 An example of page that showing responsibility of selected role

View, update and delete of other attributes are done similarly.

In the last step, company can view an existing process flow chart or remove from.

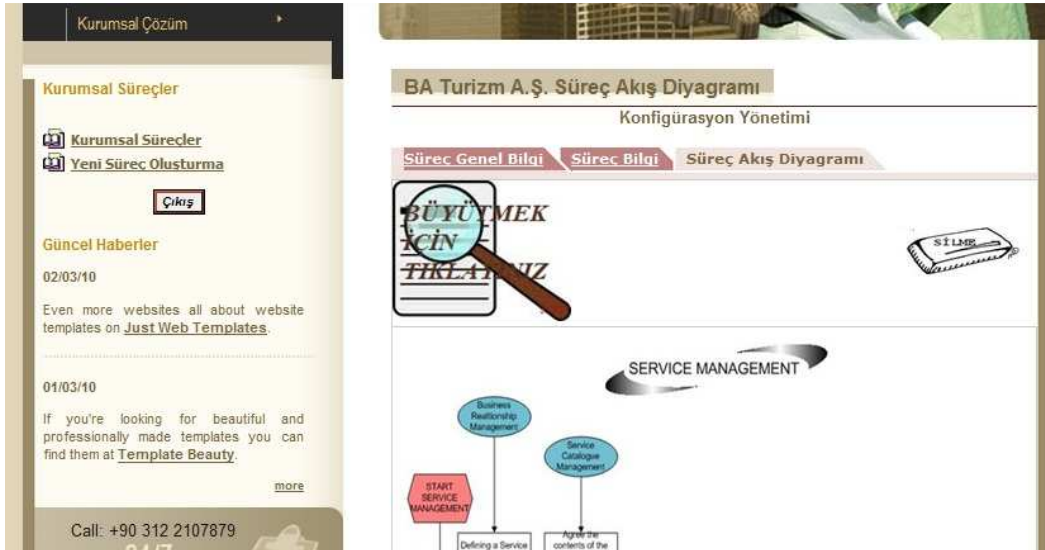


Figure 4-21 An example of page that showing flow chart of selected process

CHAPTER 5

JUSTIFICATION OF PROPOSED SOLUTION

In order to prove enforceability and effectiveness, processes are implemented in a very well known and successful organization in Ankara. Because of keeping the confidence of organization, during this chapter, organization name is stated as AB Organization.

AB is a military based organization who has a internal IT service provider named as Information Management Directorship (IMD). All services are delivered by IMD to their staffs. IMD consists of approximately seventy five employees. It has own service desk application developed by themselves which are expanded during this study named as Service Management System.

While implementing processes in organization, some small processes are combined and one of them has not been implemented yet. The underlying reason is that each organization has its own culture, approach and needs also IMD has not sufficient personnel to implement each process separated and another important reason is the time restriction of thesis. This chapter provides firstly implemented procedures by comparing the process generated in the scope of thesis. Afterward, the results of implementation of processes are explained.

5.1 Implemented Processes and Results

Any organization who has business services supported by IT services need IT processes to manage their IT services efficiently and effectively so their business services. Organization AB has an internal IT supporting business services. Fifteen processes are defined; IT Management, Service Management, IT Infrastructure Management, Risk and Information Security Management, Process Quality Management, Corporate Architecture Management, Supplier Management, Human Resources, Project Management, Incident Management, Request Management, Change Management, Software Lifecycle and Test Management for IMD. All processes are documented named as department guideline instruction. All department guidelines has consistent structure;

- Goal
- Scope
- Definitions and Abbreviation
- Related Application Documents
- Role and Responsibilities
- Inputs
- Outputs
- Flow Diagram
- Method
- Performance Metrics
- Appendixes

Alignment of all these processes implemented to IMD and processes defined in the scope of thesis is given in the table 5.1.

Table 5-1 Processes implemented in IMDB and defined in the proposed model

Processes in proposed framework	Processes implemented to IMD of AB Organization
IT Management	IT Management
Portfolio Management	IT Management
Financial Management	IT Management
Corporate Architecture	Corporate Architecture
Risk Management	Risk and Information Security Management
Software Development Lifecycle	Software Development Lifecycle
Service Level Management	Service Management
Service Catalogue Management	Service Management
Configuration Management	IT Infrastructure Management
Capacity Management	IT Infrastructure Management
Continuity Management	IT Infrastructure Management
Availability Management	IT Infrastructure Management
Event Management	IT Infrastructure Management
Information Security Management	Risk and Information Security Management
Supplier Management	Supplier Management
Human Resources Management	Human Resources Management
Project Management	Project Management
Change Management	Change Management
Release and Deployment Management	Release and Deployment Management
Test Management	Test Management
Knowledge Management	-
Request Management	Request Management
Incident Management	Incident Management
Problem Management	Incident Management
Quality Management	Quality Management

As seen in the above table, except knowledge management process which is implemented slightly, all processes are implemented in IMD of AB Organization however, some of them are combined.

The reason why knowledge management process has not been implementing yet is the need of high maturity level of it. The organization in low maturity level does not understand Knowledge Management (KM) subject however organizations with high maturity level are apt to introduce KM practices [56]. Since, the organization which processes are implemented is not in high maturity level to apply knowledge management process in a restricted and short time.

Since, AB organization is quite small and few staff, some processes are merged while implementing. Just because, some processes related to each other are owned and operated by same staffs like configuration management, capacity management and continuity management are all owned and operated by same group in IMD.

All processes are implemented and have been in final reviews by AB organization. To finish all the processes implementation, it has been waited to finish service management system (extension of service desk application) which is being developed by IMD software team.

In addition to this, since there has not been baseline numerical information, IMD has not compared themselves with the previous results yet. Because of these reasons, the statistical results are not handled yet.

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Conclusion

Organizations which have IT services have to manage their IT because of the reducing failures generated by IT. Since 1991, IT Governance has started to become more important and wide spread around the world as stated in Chapter 1 and 2. Due to this reason, so much standards or frameworks arise. As an example, COBIT is an important framework used by a great deal of companies. Also with IT Infrastructure library, IT services management has also come into prominence.

However, these standards are complementary rather than competitors. So, most organizations start to ask on their own which standards are used for their companies or which framework should be first implemented? Also, implementation of COBIT is also hard for organizations because COBIT only provides what the organization should do but not explain how. Besides, ITIL is too long and complicated to implement it and is not comprehensive like COBIT.

In the scope of thesis, new processes aligned with ITIL and COBIT to match requirements of both is defined. These processes can also include CMMI up to level 2 by adding some more requirements. In addition to these, ISO 27001's management is also added to Information Security process. All this processes are also translated to

Turkish to create knowledge bank for Turkish companies and provide a web based application for companies to manage their own processes for their organizations.

The main focus of this study is to provide IT processes which are completely based on ITIL processes if any and COBIT control objectives where processes defined in ITIL do not supply. By implementing new processes, organization automatically implement COBIT and ITIL requirements for IT.

Another aim is to reduce ITIL' sophistication and scattered and COBIT's shallow for organizations. This study helps organizations to implement IT processes easily. By giving the relation between ITIL and new processes and COBIT and new processes help the organization to follow the content of COBIT and ITIL also.

Third focus of this study is providing a web based application prepared in Turkish for Turkish companies to increase the usability of the standards/frameworks for IT. Since expect ISO 27001:2005, there is no standard / framework translated to Turkish for IT, this application firstly provides processes in Turkish to increase understandably. Also application provides organizations in Turkish to manage their processes easily in two points of views;

1. by preparing knowledge bank in Turkish,
2. by preparing a dynamic application to manage their processes.

6.2 Future Work

1. All processes' activities can be extended technically by giving more information about how to use the configuration management tool or service desk tool detail.
2. New processes added or existing processes are extended to meet engineering level of CMMI i.e. CMMI level 3.

3. Existing processes can also be aligned with very well known frameworks/standards such as PMI, ISO 20000 or PRINCE.
4. ITPG can be prepared by different languages especially in English to be used internationally.
5. The first stage of commercializing these processes is given to TÜBİTAK as a research and development project. Under this project, it can be extended such that assessment and measurement of the processes can be put in.
6. To measure organization compliance to each process, there should be a set of questions which organization can easily understand where the organization are and to realize the gap between their own processes and the best practice processes.

REFERENCES

- [1] Agarwal, R. & Sambamurthy, V. (2002) Principles and Models for Organizing the IT Function. *MIS Quarterly Executive*, (1:1), pp. 1-16.
- [2] Strassmann. P. A. (1997). *The Squandered Computer—Evaluating the Business Alignment of Information Technologies*. New Canaan: Information Economics Press.
- [3] Marshall, P. & McKay, J. (2004). Strategic IT planning, evaluation and benefits management: The basis for effective IT governance. *Australasian Journal of Information Systems*, Vol. 11, No. 2, 14-26.
- [4] Willcocks, L. (1994). Introduction: of capital importance. In Leslie Willcocks (Ed), *Information Management: The evaluation of information systems investments* (pp. 1-27). Chapman & Hall, London.
- [5] Symons, C., Cecere, M., Young, G. & Lamberd, N. (2005). *IT Governnace Framework, Structures, Processes, And Communication*. Cambridge, MA: Forrester Research, Inc. 36563.
- [6] Larsen, M. H., Pedersen, M. K. & Andersen, K. V. (2006). IT Governance: Reviewing 17 IT Governance Tools and Analysing the Case of Novozymes A/S. In *HICSS 2006: Proceedings of the 39th Annual Hawaii International Conference on System Sciences*. Washington, DC, USA: IEEE Computer Society.
- [7] Ross, J. & Weill, P. (2004). Recipes for Good Governance, *CIO:Australia's Magazine for Information Executives*, 17:4, p. 1.
- [8] Brown, A. E. & Grant, G. G. (2005). Framing the Frameworks: A Review pf IT Governance Research. *Communication of the Assoc. Inf. Syst.* 15, 696-712.
- [9] Cater-Steel, A., Tan, W-G. & Toleman, M. (2006). Challenge of Adopting Multiple

Process Improvement Frameworks. In: 14th European Conference on Information Systems (ECIS 2006), 12-14 June 2006, Goteborg, Sweden.

[10] Hayden, L. (2009). Designing Common Control Frameworks: A Model for Evaluating Information Technology Governance, Risk, and Compliance Control Rationalization Strategies. *Information Security Journal: A Global Perspective*, Vol. 18, No. 6, 297-305.

[11] Callahan, J. & Keyes, D. (2003). The Evolution of IT Governance at NB Power. In W. Van Grembergen (Ed.), *Strategies for Information Technology Governance*. Hershey, PA: Idea Group Publishing.

[12] Morency, J. (2005). Best practice, practice, practice, *Network World*, Retrieved June 23, 2010 from <http://www.networkworld.com/research/2005/011005cobit.html>

[13] Cater-Steel, A., Toleman, M. & Tan, W-G. (2006). Transforming IT Service Management – the ITIL Impact. Proceedings of the 17th Australasian Conference on Information Systems - ACIS. Adelaide, Australia, 6-8 December.

[14] Calder, A. (2005). *The Case for ISO 27001*. IT Governance Institute.

[15] Calder, A. (2006). Information Security and ISO 27001 - an Introduction. IT Governance Institute, 1-6.

[16] Broderick, J. S. (2006). ISMS, security standards and security regulations. *Information Security Technical Report*, Vol. 11, Issue 1, 26-31.

[17] Hardy, G. (2006). Guidance on Aligning COBIT, ITIL and ISO 17799. *Information Systems Control Journal*, Vol. 1, p. 32-33.

[18] von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, Vol. 24, pp. 99-104.

[19] Curtis, B. (2005). Integrating CMMI with COBIT and ITIL. Borland

- [20] Wallhoff, J. (2004). Combining ITIL with COBIT and ISO/IEC 17799:2000. Whitepaper, Scillani Information AB. Retrieved June 10, 2010, from <http://www.scillani.com>.
- [21] TBD Kamu – BİB Kamu Bilişim Platformu. (2008). *Bilişim Teknolojilerinde Yönetişim*. Ankara
- [22] Control Objectives for Information Technology. (2007). United States of America: IT Governance Institute (ITGI).
- [23] Weill, P. & Woodham, R. (2002). Don't Just Lead, Govern: Implementing Effective IT Governance (CISR Working Paper No. 326). Center for Information Systems Research, MIT Sloan School of Management. Retrieved June 10, 2010, from Massachusetts Institute of Technology Web site: <http://dspace.mit.edu/bitstream/1721.1/1846/2/4237-02.pdf>
- [24] IT Governance Institute (2006). IT Governance Global status Report - 2006. ITGI and PricewaterhouseCoopers. Available from www.itgi.org
- [25] Hussain, S. J. & Siddiqui, M. S. (2005). Quantified Model of COBIT for Corporate IT Governance. In First International Conference on Information and Communication Technologies, pp. 158 – 163, IEEE, Los Alamitos.
- [26] von Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security*, Vol. 7, Issue 1, pp. 50-58.
- [27] Choi, W., & Yoo, D. (2009). Assessment of IT Governance of COBIT Framework. *Communications in Computer and Information Science*, Vol. 62, pp. 82-89.
- [28] IT Infrastructure Library - Service Strategy. (2007). United Kingdom: The Stationary Office.
- [29] Sallé, M. (2004). IT Service Management and IT Governance: review, comparative analysis and their impact on utility computing. Hewlett-Packard Company.
- [30] Galup, S., Dattero, R., Quan, J. & Conger, S. (2009). An Overview of Information Technology Service Management. *Communications of the ACM*, Vol. 52, No. 5, pp. 124-127.

[31] Roux, Y. L. (2005). Using ISO 17799, COBIT & ITIL for solving Compliance Issue, Paulus, S., Pohlmann, H., & Reimer, H. (Eds.), ISSE 2005 Securing Electronic Business Processes (pp. 313-323) Computer Associates Int.

[32] Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Windebank, J. & Rance, S. (2007). An Introductory Overview of ITIL V3 (Cartlidge, A. and Lillycrop, M. Ed.). The UK Chapter of IT Service Management Forum (itSMF), Wokingham

[33] Potgieter, B.C., Botha, J.H., & Lew, C. (2005). Evidence that use of the ITIL framework is effective. 18th Annual Conference of the National Advisory Committee on Computing Qualifications. Tauranga, NZ., pp. 160-167.

[34] McLaughlin, K. & Fred, D. (2007). American ITIL. Proceedings of the 35th Annual ACM SIGUCCS fall conference. Orlando, Florida, USA. Pp. 251-254.

[35] IT Infrastructure Library - Service Design. (2007). United Kingdom: The Stationary Office.

[36] IT Infrastructure Library - Service Operation. (2007). United Kingdom: The Stationary Office.

[37] IT Infrastructure Library - Service Transition. (2007). United Kingdom: The Stationary Office.

[38] IT Infrastructure Library – Continual Service Improvement. (2007). United Kingdom: The Stationary Office.

[39] Huang, S.-J., & Han, W.-M. (2005). Selection priority of process areas based on CMMI continuous representation. *Information & Management* , 297-307.

[40] Alho, K. (2006). 10 Common Misconceptions about CMMI. Retrieved June 10, 2010 from <http://www.improveit.fi/docs/10Misconceptions.pdf>

[41] Eloff, M. M., & von Solms, S. H. (2000). Information Security Management: A Hierarchical for Various Approaches. *Computers & Security*, Vol. 19, No. 3, pp. 243 - 256.

[42] Calder, A. (2006). *Information Security Based on ISO 27001/ ISO 17799*. Van Haren.

[43] Eloff, J. H. P. & Eloff, M. (2003). Information Security Management – A New paradigm. In: Proceedings of the 2003 annual research conference of the South African Institute of Computer Scientists and Information Technologist on enablement through technology SAICSIT, pp. 130-136.

[44] Eloff, J. H. P., & Eloff, M. (2005). Integrated Information Security Architecture. Computer Fraud and Security, Vol.11, pp. 10-16.

[45] Humphreys, T. (2006). State-of-the-art information security management systems with ISO/IEC 27001:2005. ISO Management Systems, pp. 15-18.

[46] Da Cruz, E. & Labuschagne, L. (2006). A New Framework For Bridging The Gap Between It Service Management And It Governance From A Security Perspective. Academy of Information Technology at the University of Johannesburg . Retrieved June 10, 2010 from http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/072_Article.pdf

[47] Mingay, S. & Bittinger, S. (2002). Combine CobiT and ITIL for Powerful Governance (No. TG-16-1849). Gartner Inc.

[48] Hoekstra, A. & Conradie, N. (2002). CobiT, ITIL and ISO17799 How to use them in conjunction. Retrieved June 10, 2010 from http://www.cccure.org/Documents/COBIT/COBIT_ITIL_and_BS7799.pdf.

[49] Hill, P. & Turbitt, K. (2006). Combine ITIL and COBIT to Meet Business Challenges. BMC Software. Retrieved July 23, 2010 from http://www.smcgltd.com/files/documents/bmc_bpwp_ital_cobit_06.pdf

[50] Rob, E. (2007). ITIL is the hitchhiker's guide, COBIT is the encyclopaedia. Retrieved from The IT Skeptic: <http://www.itskeptic.org/node/423>

[51] Comparison between COBIT, ITIL and ISO 27001. Retrieved July 23, 2010 from Security Procedure Information System Auditing Resources:
<http://www.securityprocedure.com/comparison-between-cobit-til-and-iso-27001>

[52] Tom, P. (2007). ITIL, COBIT, and Sarbanes-Oxley. Retrieved August 11, 2010 from <http://www.enterpriseleadership.org/blogs/Articles/2007/12/05/til-cobit-and-sarbanes-oxley>

[53] *COBIT Quickstart 2. Edition.* (2007). United States of America: IT Governance Institute.

[54] *Mapping of ITIL V3 with COBIT 4.1.* (2008). United States of America, Rolling Meadows: ISACA & ITGI

[55] Lo, R., & Richards, B. (2009). ITIL® v3 Knowledge Management Why this new process is more than just your knowledge base. ThirdSky, pp. 1-32.

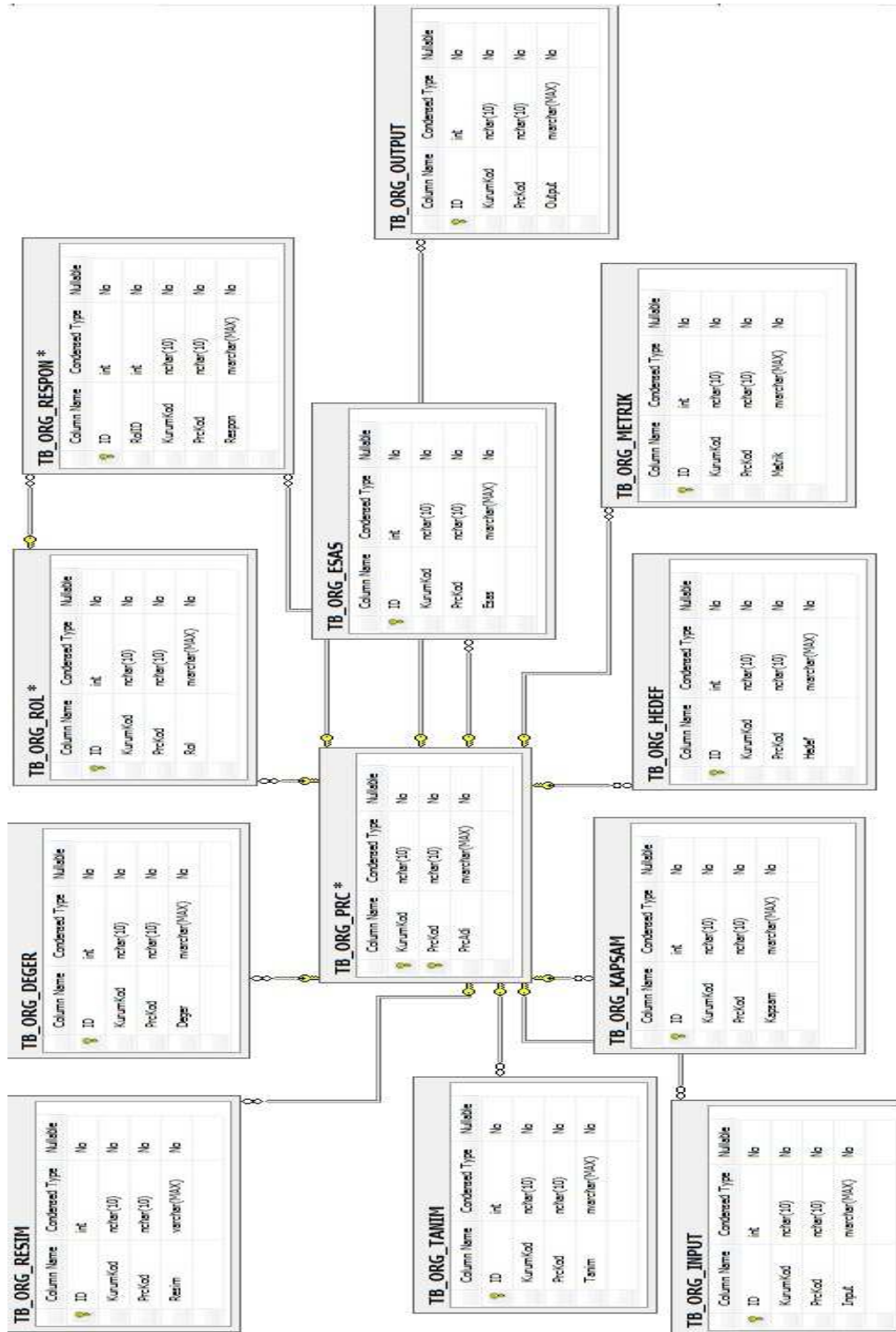
[56] Sepulveda, J. M., & Tapia, G. G. A Framework For Evaluation And Prioritization Of Knowledge Management Initiatives By An Analytical Network Process. Proceedings of 19th International Conference on Production Research, pp. 1-8. Santiago-Chile.

APPENDICES

APPENDIX A – The Service Design Package Content

Category	Sub-Category
Requirements	Business requirements
	Service applicability
	Service contacts
Service Design	Service functional requirements
	Service level requirements
	Service and operational management requirements
	Service design and topology
Organizational Readiness Assessment	Organizational readiness assessment
Service Lifecycle Plan	Service programme
	Service transition plan
	Service operational acceptance plan
	Service acceptance criteria

APPENDIX B – Database ER Diagram



APPENDIX C – Process Documentation Template

- ✓ Process Name, description and administration
- ✓ Vision and mission statements
- ✓ Objectives
- ✓ Scope and term of reference
- ✓ Process overview
 - ❖ Description and overview
 - ❖ Inputs
 - ❖ Procedures
 - ❖ Activities
 - ❖ Outputs
 - ❖ Triggers
 - ❖ Tools and other deliverables
 - ❖ Communication
- ✓ Roles and Responsibilities
 - ❖ Operational Responsibilities
 - ❖ Process owner
 - ❖ Process members
 - ❖ Process users
 - ❖ Other roles
- ✓ Associated documentation and references
- ✓ Interfaces and dependencies to:
 - ❖ Other SM processes
 - ❖ Other IT processes
 - ❖ Business processes

- ✓ Process measurement and metrics: reviews, assessments and audits
- ✓ Deliverables and reports produced by the process
 - ❖ Frequency
 - ❖ Content
 - ❖ Distribution
- ✓ Glossary, acronyms and references

APPENDIX D – Sample SLA and OLA

SERVICE LEVEL AGREEMENT (SLA – SAMPLE)

The agreement is made between..... and
.....

This document covers the provision and support of services
which.....

The agreement remains valid for time from the (date) to (date).

Signatories;

Name.....Position.....Date.....
.....

Name.....Position.....Date.....
.....

Service Description:

Service Hours:

Service Availability:

Reliability:

Customer support:

Contact points and escalation:

Service performance:

Batch turnaround times:

Functionality (if appropriate):

Change Management:

Service Continuity:

Security:

Printing:

Responsibilities:

Charging (if applicable):

Service reporting and reviewing:

Glossary:

Amendment sheet:

OPERATIONAL LEVEL AGREEMENT (OLA – SAMPLE)

The agreement is made between..... and
.....

This document covers the provision of the support service providing
.....

The agreement remains valid for time from the (date) to (date).

Signatories;

Name.....Position.....Date.....
.....

Name.....Position.....Date.....
.....

Details of previous amendments:

Support service description:

Scope of the agreement:

Service hours:

Service targets:

Contact points and escalation:

Service desk and incident response times and responsibilities:

Problem response times and responsibilities:

Change Management:

Release Management:

Configuration Management:

Information Security Management:

Availability Management:

Service Continuity Management:

Capacity Management:

Service Level Management:

Supplier Management:

Provision of information:

Glossary:

Amendment sheet:

APPENDIX E – Service Catalogue Example

Service Name	Service Description	Service type	Supporting services	Business Owner(s)	Business Unit(s)	Service Manager(s)	Business Impact
Service 1							
Service 2							
Service 3							

Business Priority	SLA	Service Hours	Business Contacts	Escalation Contacts	Service Reports	Service Reviews	Security Rating

APPENDIX F – Statement of Requirements (SoR) and/or Invitation to Tender (ITT)

- ✓ A description of the services, products and/or components required
- ✓ All relevant technical specifications, details and requirements
- ✓ An SLR where applicable
- ✓ Availability, reliability, maintainability and serviceability requirements
- ✓ Details of ownership of hardware, software, buildings, facilities, etc.
- ✓ Details of performance criteria to be met by the equipment and supplier(s)
- ✓ Details of all standards to be complied with (internal, external, national and international)
- ✓ Legal and regulatory requirements
- ✓ Details of quality criteria
- ✓ Contractual timescales, details and requirements, terms and conditions
- ✓ All commercial considerations: costs, charges, bonus and penalty payments and schedules
- ✓ Interfaces and contacts required
- ✓ Project management methods to be used
- ✓ Reporting, monitoring and reviewing procedures and criteria to be used during and after the implementation
- ✓ Supplier requirements and conditions
- ✓ Sub-contractor requirements
- ✓ Details of any relevant terms and conditions
- ✓ Description of the supplier response requirements
 - ❖ Format
 - ❖ Criteria

- ❖ Conditions
- ❖ Timescales
- ❖ Variances and omissions
- ❖ Customer responsibilities and requirements
- ✓ Details of planned and possible growth
- ✓ Procedures for handling change
- ✓ Details of the contents and structure of the responses required

APPENDIX G – Capacity Plan Sample

CAPACITY PLAN CONTENT

- 1. Introduction**
 - 2. Management Summary**
 - 3. Business Scenarios**
 - 4. Scope and Terms of Reference of the Plan**
 - 5. Methods Used**
 - 6. Assumptions Made**
 - 7. Service Summary**
 - 8. Resource Summary**
 - 9. Options for Service Improvement**
 - 10. Cost Forecast**
 - 11. Recommendations**
-

APPENDIX I – Definitions

Activity : A set of actions to achieve a particular result

Agreement (SLM) : An illegal document that binds two or more parties to specific and implied obligations

Alert :(Event Management) A warning that a threshold has been reached, something as changed or failure has occurred

Application (Software Development): It is a kind of software development that provides functions

Architecture (Organization Architecture): Design, or the way components fit together. It can be used to describe any system or IT service, as in "organizational architecture"

Asset (Capacity Management): Any resource of capability. It can be any type of management, organization, people, etc.

Audit (Configuration Management): Review of the records, targets or guideline/standard to check whether they are accurate, met or followed respectively.

Backup (Risk and Continuity Management): Making copy of important files to protect against loss

Baseline : A benchmark used as a reference point

Benchmark (Quality Management): Current situation recorded at any time

Budget (Financial Management): Planned intended expenditures and income for a defined period of time

Business Case : Justification for a significant item of expenditure

Business Relationship Management : The process or function that provides a communication with business.

Business Unit : A part of business that has own plan, cost, input and metrics

Capacity (Capacity Management): The maximum throughput of a CI or IT service can deliver

Change (Change Management): Addition, modification or removal from IT service

Charging (Financial Management): The price demanded for IT services

Configuration (Configuration Management): A specification of IT services i.e. a group of configuration items that work together

Configuration Item (Configuration Management): An asset, service component or other item that is, or will be, under the control of Configuration Management.

Configuration baseline: Configuration of a service, product or infrastructure that has been formally reviewed and agreed on, that thereafter serves as the basis for further activities and that can be changed only through formal change procedures.

Contract (Supplier Management): A legal agreement between two or more parties

Cost (Financial Management): The amount of money spent on activity, IT service

Diagnosis (Incident Management): to identify the workaround for incident or root cause of problem

Directory service (Security Management and Risk Management):

Escalation (Incident, Problem Management): The act of advancing an issue to the next appropriate level for resolution, types are functional and hierarchical

Event (Event Management): A Change of a state that has significance for the management of CI or Service

External service provider: IT service provider part of a different organization

Function : A team of ser of people and tools they use to realize processes or activities

Help Desk (Service Desk): A point of customers or users to contact for service request or incident logging

Incident (Incident Management): An unplanned interruption to It service or reduction in the quality of service

IT Infrastructure (IT Infrastructure Management):: All of the hardware, software, networks, facilities, etc. are used to support IT services.

IT Service : A service that is provided to one or more customers by IT service providers

IT Service Provider: A service provider that provides IT services

Knowledge base (Knowledge Management): A database containing the data

Maturity (Quality Management): A measure of the processes, functions, organizations, etc.

Net Present Value (Financial Management): A technique used to make help decisions about capital expenditure

OLA : Operational Level Agreement is an agreement between an IT service provider and another part of the same organization that assists with the provision of services.

Organization : A company, legal entity or other institution

Pricing (Financial Management): The activity for establishing how much customers will be charged

Priority : A category used to define relative importance of incident, problem or change

Problem (Problem Management): A cause of one or more incidents

Process : A structured set of activities designed to accomplish a specific objective.

Programme (Project Management): Planned or managed a set of projects or activities

Project (Project Management): A temporary organization to achieve an objective containing people, asset and having a lifecycle.

Quality (Quality Management): Denote the degree of perfection of a product, service or process in terms of the intended value

Recovery (Continuity Management): Returning a Configuration item or service to a working state

Release (Release and Deployment Management): A collection of hardware, software, documentation, process or components required for IT services to deploy into live environment

Release Unit (Release and Deployment): Components of an IT service released together. A release unit includes enough components to perform a useful function

Requirement (Software Lifecycle): Formal statement stating a business or technical demand

Resource (IT Infrastructure Management): Including IT Infrastructure, people, money or anything else that helps to deliver IT service

Response Time (Availability Management):

Restore (Continuity Management): To recall a previously used state after recovery or repair from an Incident

Retire (Release and Deployment Management): Removal of an IT service or Configuration item from live environment

ROI (Financial Management): A measurement of the expected benefit of an investment

Risk (Risk Management): A possible event that can cause or destroy or affect the ability to achieve objectives

Role : A person or a team that has some responsibilities, activities or authorities

Scope : The breadth, boundary, depth or extent of a subject

Secure Library : Collection of software, electronic or document CIs of known type and status.

Server (IT Infrastructure Management): A computer that is responsible for responding to requests made by a client program providing software functions

Service (Event Management): A means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks

SLA : Service Level Agreement is a written agreement between an IT service provider and the IT customer(s), defining the Key service targets and responsibilities of both parties.

Stakeholder : All people who have an interest in organization, project service, IT service, etc.

Strategy (IT Management): A careful plan or method to achieve defined objectives

Supplier (Supplier Management): A vendor who provides goods or services that are required to deliver IT service

System : A number of related things that work together to achieve an objective

Test (Test Management): An activity that verifies a service or configuration item meets specification or requirements

Third party (Supplier Management): Suppliers

Threat (Security Management): Anything that might exploit vulnerability

Threshold (Event Management): The level of a system process at which sudden or rapid change occurs

Throughput (IT Infrastructure Management): A measure of the number of transactions or operations in fixed time

Underpinning Agreements: OLAs, SLAs and contracts

Use Case (Software Lifecycle): A technique used to figure out functionality or objectives

Variance (Financial Management): The differences between planned value and actual measured value

Version : Identification of a specific baseline of a configuration item

Vision (IT Management): A statement that describes how the organization intends to become in the future

APPENDIX J – Mapping Framework with COBIT 4.1

P.1 IT Management	PO1.2 Business-IT Alignment PO1.3 Assessment of Current Capability and Performance PO1.4 IT Strategic Plan PO1.5 IT Tactical Plans PO4.1 IT Process Framework PO4.2 IT Strategy Committee PO4.3 IT Steering Committee PO4.4 Organizational Placement of the IT Function PO4.5 IT Organizational Structure PO4.8 Responsibility for Risk, Security and Compliance PO4.10 Supervision PO4.11 Segregation of Duties PO4.14 Contracted Staff Policies and Procedures PO4.15 Relationships PO6 Communicate Management Aims and Direction
P.2 Portfolio Management	PO1.2 Business-IT Alignment PO1.5 IT Tactical Plans PO1.6 IT Portfolio Management
P.3 Financial Management	PO5 Manage the IT Investment DS6 Identify and Allocate Costs
P.4 Request Management	PO8.4 Customer Focus DS5.3 Identity Management DS5.4 User Account Management
P.5 Corporate Architecture	PO3 Determine Technological Direction
P.6 Risk Management	PO9 Assess and Manage IT Risks AI1.2 Risk Analysis Report DS4.9 Offsite Backup Storage DS11.6 Security Requirements for Data Management

P.7 Software Development Lifecycle Management	AI1.1 Definition and Maintenance of Business Functional and Technical Requirements AI2.1 High-level Design AI2.2 Detailed Design AI2.3 Application Control and Auditability AI2.4 Application Security and Availability AI2.6 Major Upgrades to Existing Systems AI2.7 Development of Application Software AI2.9 Applications Requirements Management AI2.10 Application Software Maintenance
P.8 Service Level Management	DS1.1 Service Level Management Framework DS1.3 Service Level Agreements DS1.4 Operating Level Agreements DS1.5 Monitoring and Reporting of Service Level Achievements DS1.6 Review of Service Level Agreements and Contracts
P.9 Service Catalogue Management	DS1.2 Definition of Services DS6.1 Definition of Services
P.10 Configuration Management	DS9 Manage the Configuration DS10.4 Integration of Configuration, Incident and Problem Management
P.11 Capacity Management	DS3.1 Performance and Capacity Planning DS3.2 Current Performance and Capacity DS3.3 Future Performance and Capacity DS3.5 Monitoring and Reporting
P.12 Continuity Management	DS4.1 IT Continuity Framework DS4.2 IT Continuity Plans DS4.2 IT Continuity Plans DS4.3 Critical IT Resources DS4.4 Maintenance of the IT Continuity Plan DS4.5 Testing of the IT Continuity Plan DS4.6 IT Continuity Plan Training DS4.7 Distribution of the IT Continuity Plan DS4.8 IT Services Recovery and Resumption DS4.10 Post-resumption Review
P.13 Availability Management	DS3.4 IT Resources Availability DS3.5 Monitoring and Reporting
P.14 Event Management	DS3.2 Current Performance and Capacity DS13.3 IT Infrastructure Monitoring

P.15 Information Security Management	AI1.2 Risk Analysis Report DS5 Ensure Systems Security DS11.6 Security Requirements for Data Management
P.16 Supplier Management	AI5 Procure IT Resources DS2 Manage Third-party Services
P.17 Human Resources Management	DS7 Educate and Train Users PO4.6 Establishment of Roles and Responsibilities PO4.12 IT Staffing PO4.13 Key IT Personnel PO7 Manage IT Human Resources
P.18 Project management	PO10 Manage Projects
P.19 Change Management	AI6 Manage Changes DS9.3 Configuration Integrity Review
P.20 Release and Deployment Management	AI7.1 Training AI7.3 Implementation Plan AI7.5 System and Data Conversion AI7.8 Promotion to Production AI7.9 Post-implementation Review
P.21 Test Management	AI7.2 Test Plan AI7.4 Test Environment AI7.6 Testing of Changes AI7.7 Final Acceptance Test AI3.4 Feasibility Test Environment
P.22 Knowledge Management	PO2.1 Enterprise Information Architecture Model PO2.2 Enterprise Data Dictionary and Data Syntax Rules PO2.3 Data Classification Scheme PO2.4 Integrity Management PO4.9 Data and System Ownership AI4.2 Knowledge Transfer to Business Management AI4.3 Knowledge Transfer to End Users AI4.4 Knowledge Transfer to Operations and Support Staff DS11.1 Business Requirements for Data Management DS11.2 Storage and Retention Arrangements DS11.3 Media Library Management System DS11.4 Disposal DS11.5 Backup and Restoration

P.23 Incident Management	DS8.2 Registration of Customer Queries DS8.3 Incident Escalation DS8.4 Incident Closure DS8.5 Reporting and Trend Analysis DS9.3 Configuration Integrity Review DS10.4 Integration of Configuration, Incident and Problem Management
P.24 Problem Management	DS9.3 Configuration Integrity Review DS10 Manage Problems
P.25 Quality Management	ME1 Monitor and Evaluate IT Performance ME2 Monitor and Evaluate Internal Control ME3 Ensure Compliance With External Requirements PO4.7 Responsibility for IT Quality Assurance PO8 Manage Quality AI2.8 Software Quality Assurance
F.1 Service Desk	DS8.1 Service Desk DS8.2 Registration of Customer Queries DS8.5 Reporting and Trend Analysis
F.2 Application Management	PO4.9 Data and System Ownership AI1.1 Definition and Maintenance of Business Functional and Technical Requirements AI1.3 Feasibility Study and Formulation of Alternative Courses of Action AI1.4 Requirements and Feasibility Decision and Approval AI2.5 Configuration and Implementation of Acquired Application Software AI4.1 Planning for Operational Solutions DS13.1 Operations Procedures and Instructions
F.3 Technical Management	DS11.5 Backup and Restoration DS13.1 Operations Procedures and Instructions DS13.5 Preventive Maintenance for Hardware AI3 Acquire and Maintain Technology Infrastructure AI4.1 Planning for Operational Solutions
F.4 Operational Management	AI4.1 Planning for Operational Solutions

APPENDIX K – Mapping Framework with ITILV3

P.1 IT Management	SS 4.1 Define the market SS 4.4 Prepare for execution SS 6.1 Organizational development SS 6.2 Organizational departmentalization SS 6.3 Organizational design SS 6.4 Organizational culture SS 9.1 Complexity SS 9.2 Co-ordination and control SS 9.3 Preserving value SD 3.6.3 Designing technology architectures SD 3.6.4 Designing processes SD 3.11 Service design models SD 6.1 Functional roles analysis SD 6.3 Skills and attributes ST 5 Service transition common operation activities ST 6.2 Organizational context for transitioning a service ST 6.3 Organization models to support service transition ST 8 Implementing service transition SO 6.7 Service operation organization structures SO 8 Implementing service operation CSI 5.4 Measuring and reporting frameworks
P.2 Portfolio Management	SS 4.2 Develop the offerings SS 4.4 Prepare for execution SS 5.3 Service portfolio management SS 5.4 Service portfolio management methods SD 3.6 Design aspects SD 3.6.2 Designing supporting systems, especially the service portfolio
P.3 Financial Management	SS 5.1 Financial management SS 5.2 Return on investment SD 3.6 Design aspects SO 4.6.7 Financial management for IT services (as operational activities)

P.4 Request Management	SS 5.5 Demand management SO 4.3 Request fulfillment SO 4.5 Access management CSI 4.1 The seven-step improvement process
P.5 Corporate Architecture	SD 3.6.3 Designing technology architectures
P.6 Risk Management	SS 9.5 Risks SD 8.3 Risks to the services and processes CSI 5.6.3 IT service continuity management
P.7 Software Development Lifecycle Management	SS 8.1 Service automation SD 3.4 Identifying and documenting business requirements and drivers SD 3.6.1 Designing service solutions SD 3.7.3 Develop the service solution (development is just mentioned) SD 5.1 Requirements engineering SD 5.3 Application management SO 6.1 Functions SO 6.5 Application management
P.8 Service Level Management	SS 5.5 Demand management SD 8.2 Service level requirements SD 4.2 Service level management CSI 4.1 The seven-step improvement process CSI 4.6 Service level management
P.9 Service Catalogue Management	SD 4.1 Service catalogue management
P.10 Configuration Management	ST 4.3 Service asset and configuration management SO 4.6.2 Configuration management (as operational activities)
P.11 Capacity Management	SD 4.3 Capacity management SO 4.6.4 Capacity management (as operational activities) CSI 5.6.2 Capacity management
P.12 Continuity Management	SS 5.1.3.4 Business Impact Analysis SD 8.1 Business impact analysis (not in detail) SD 4.5 IT service continuity management SO 4.6.8 IT Service continuity management CSI 5.6.3 IT service continuity management
P.13 Availability Management	SS 7.5 Strategy and improvement SD 4.4 Availability management SO 4.6.5 Availability management (as operational activities) CSI 5.6.1 Availability management

P.14 Event Management	SO 4.1 Event Management SO 5.2.1 Console management/operations bridge
P.15 Information Security Management	SD 4.6 Information security management SO 4.5 Access management SO 5.4 Server management and support CSI 5.6.3 IT service continuity management
P.16 Supplier Management	SS 6.5 Sourcing strategy SD 4.7 Supplier management SD 3.7.1 Evaluation of alternative solutions SD 3.7.2 Procurement of the preferred solution
P.17 Human Resources Management	SO 5.13 Information security management and service operation (vague)
P.18 Project management	SD 3.4 Identifying and documenting business requirements and drivers ST 8 Implementing service transition
P.19 Change Management	ST 4.2 Change management ST 4.2.7 Triggers, input and output, and inter-process interfaces ST 5 Service transition common operation activities ST 5.2 Managing organization and stakeholder change SO 4.6.1 Change management (as operational activities) CSI 5.6.5 Change, release and deployment management
P.20 Release and Deployment Management	ST 4 Service transition processes ST 4.4 Release and deployment management ST 4.4.5.1 Planning ST 4.4.5.2 Preparation for build, test and deployment ST 4.4.5.5 Plan and prepare for deployment ST 4.4.5.6 Perform transfer, deployment and retirement ST 4.4.5.7 Verify deployment ST 4.4.5.8 Early life support ST 4.4.5.9 Review and close a deployment ST 4.4.5.10 Review and close service transition ST 4.6 Evaluation SO 4.6.3 Release and deployment management (as operational activities)
P.21 Test Management	ST 4.4.5.1 Planning ST 4.4.5.3 Build and test ST 4.4.5.4 Service testing and pilots ST 4.5 Service validation and testing (ITIL is not focused just on service transition, but on ongoing test

	of the service.)
P.22 Knowledge Management	SD 3.6.3 Designing technology architectures SD 5.2 Data and information management ST 4.7 Knowledge management SO 4.6.6 Knowledge management (as operational activities) SO 5.2.3 Backup and restore CSI 5.6.6 Knowledge management
P.23 Incident Management	SO 4.2 Incident management
P.24 Problem Management	SO 4.4 Problem management CSI 5.6.4 Problem management
P.25 Quality Management	SS 9.4 Effectiveness in measurement SD 8.5 Measurement of service design SD 3.6.5 Design of measurement systems and metric SO 5.1 Monitoring and control CSI Introduction CSI 2 Service management as a practice CSI 3 CSI principles CSI 4.1 The seven-step improvement process CSI 4.2 Service reporting CSI 4.3 Service measurement CSI 4.4 Return on investment for CSI 4.5 Business questions for CSI CSI 5.1 Methods and techniques CSI 5.2 Assessments CSI 5.3 Benchmarking CSI 5.5 The Deming Cycle
F.1 Service Desk	SO 6.1 Functions SO 6.2 Service desk
F.2 Technical Management	SS 8.1 Service automation SD 3.3 Identifying service requirements SD 3.4 Identifying and documenting business requirements and drivers SD 3.6.1 Designing service solutions SD 3.6.3 Designing technology architectures SD 3.7.1 Evaluation of alternative solutions SD 3.8 Design constraints SO 3.7 Documentation SO 6.5 Application management

F.3 Application Management	SD 3.3 Identifying service requirements SD 3.4 Identifying and documenting business requirements and drivers SD 3.8 Design constraints SO 3.7 Documentation SO 5.5 Network management SO 5.7 Database administration SO 5.8 Directory services management SO 5.9 Desktop support SO 5.10 Middleware management SO 5.11 Internet/web management SO 6.1 Functions SO 6.3 Technical management
F.4 Operational Management	SO 3.7 Documentation SO 5.1 Monitoring and control SO 5.2 IT operations SO 5.2.2 Job scheduling SO 5.2.3 Backup and restore SO 5.2.4 Print and output SO 5.3 Mainframe management SO 5.4 Server management and support SO 5.6 Storage and archive SO 5.12 Facilities and data centre management SO 6.1 Functions SO 6.4 IT operations management SO 6.4 IT operations management

APPENDIX L – Mapping COBIT 4.1 with Framework

PO1 Define a Strategic IT Plan	
PO1.1 IT Value Management	All processes
PO1.2 Business-IT Alignment	P.1 IT Management P.2 Portfolio Management
PO1.3 Assessment of Current Capability and Performance	P.1 IT Management
PO1.4 IT Strategic Plan	P.1 IT Management
PO1.5 IT Tactical Plans	P.1 IT Management P.2 Portfolio Management
PO1.6 IT Portfolio Management	P.2 Portfolio Management
PO2 Define the Information Architecture	
PO2.1 Enterprise Information Architecture Model	P.21 Knowledge Management
PO2.2 Enterprise Data Dictionary and Data Syntax Rules	P.21 Knowledge Management
PO2.3 Data Classification Scheme	P.21 Knowledge Management
PO2.4 Integrity Management	P.21 Knowledge Management
PO3 Determine Technological Direction	
PO3.1 Technological Direction Planning	P.4 Corporate Architecture
PO3.2 Technology Infrastructure Plan	P.4 Corporate Architecture
PO3.3 Monitor Future Trends and Regulations	P.4 Corporate Architecture
PO3.4 Technology Standards	P.4 Corporate Architecture
PO3.5 IT Architecture Board	P.4 Corporate Architecture
PO4 Define the IT Processes, Organization and Relationships	
PO4.1 IT Process Framework	P.1 IT Management
PO4.2 IT Strategy Committee	P.1 IT Management
PO4.3 IT Steering Committee	P.1 IT Management
PO4.4 Organizational Placement of the IT Function	P.1 IT Management
PO4.5 IT Organizational Structure	P.1 IT Management
PO4.6 Establishment of Roles and Responsibilities	P.16 Human Resources Management
PO4.7 Responsibility for IT Quality Assurance	Quality Management
PO4.8 Responsibility for Risk, Security and	P.1 IT Management

Compliance	
PO4.9 Data and System Ownership	P.21 Knowledge Management Application Management
PO4.10 Supervision	P.1 IT Management
PO4.11 Segregation of Duties	P.1 IT Management
PO4.12 IT Staffing	P.16 Human Resources Management
PO4.13 Key IT Personnel	P.16 Human Resources Management
PO4.14 Contracted Staff Policies and Procedures	P.1 IT Management
PO4.15 Relationships	P.1 IT Management
PO5 Manage the IT Investment	
PO5.1 Financial Management Framework	P.3 Financial Management
PO5.2 Prioritization Within IT Budget	P.3 Financial Management
PO5.3 IT Budgeting	P.3 Financial Management
PO5.4 Cost Management	P.3 Financial Management
PO5.5 Benefit Management	P.3 Financial Management
PO6 Communicate Management Aims and Direction	
PO6.1 IT Policy and Control Environment	P.1 IT Management
PO6.2 Enterprise IT Risk and Control Framework	P.1 IT Management
PO6.3 IT Policies Management	P.1 IT Management
PO6.4 Policy, Standard and Procedures Rollout	P.1 IT Management
PO6.5 Communication of IT Objectives and Direction	P.1 IT Management
PO7 Manage IT Human Resources	
PO7.1 Personnel Recruitment and Retention	P.16 Human Resources Management
PO7.2 Personnel Competencies	P.16 Human Resources Management
PO7.3 Staffing of Roles	P.16 Human Resources Management
PO7.4 Personnel Training	P.16 Human Resources Management
PO7.5 Dependence Upon Individuals	P.16 Human Resources Management
PO7.6 Personnel Clearance Procedures	P.16 Human Resources Management
PO7.7 Employee Job Performance Evaluation	P.16 Human Resources Management

PO7.8 Job Change and Termination	P.16 Human Resources Management
PO8 Manage Quality	
PO8.1 Quality Management System	P.25 Quality Management
PO8.2 IT Standards and Quality Practices	P.25 Quality Management
PO8.3 Development and Acquisition Standards	P.25 Quality Management
PO8.4 Customer Focus	P.8 Service Level Management P.22 Request Management P.25 Quality Management
PO8.5 Continuous Improvement	P.25 Quality Management
PO8.6 Quality Measurement, Monitoring and Review	P.25 Quality Management
PO9 Assess and Manage IT Risks	
PO9.1 IT Risk Management Framework	P.5 Risk Management
PO9.2 Establishment of Risk Context	P.5 Risk Management
PO9.3 Event Identification	P.5 Risk Management
PO9.4 Risk Assessment	P.5 Risk Management
PO9.5 Risk Response	P.5 Risk Management
PO9.6 Maintenance and Monitoring of a Risk Action Plan	P.5 Risk Management
PO10 Manage Projects	
PO10.1 Programme Management Framework	P.17 Project Management
PO10.2 Project Management Framework	P.17 Project Management
PO10.3 Project Management Approach	P.17 Project Management
PO10.4 Stakeholder Commitment	P.17 Project Management
PO10.5 Project Scope Statement	P.17 Project Management
PO10.6 Project Phase Initiation	P.17 Project Management
PO10.7 Integrated Project Plan	P.17 Project Management
PO10.8 Project Resources	P.17 Project Management
PO10.9 Project Risk Management	P.17 Project Management
PO10.10 Project Quality Plan	P.17 Project Management
PO10.11 Project Change Control	P.17 Project Management
PO10.12 Project Planning of Assurance Methods	P.17 Project Management
PO10.13 Project Performance Measurement, Reporting and Monitoring	P.17 Project Management
PO10.14 Project Closure	P.17 Project Management
AI1 Identify Automated Solutions	
AI1.1 Definition and Maintenance of Business Functional and Technical Requirements	F.2 Application Management P.6 Software Development Lifecycle

AI1.2 Risk Analysis Report	P.5 Risk Management P.14 Information Security Management
AI1.3 Feasibility Study and Formulation of Alternative Courses of Action	F.2 Application Management
AI1.4 Requirements and Feasibility Decision and Approval	F.2 Application Management
AI2 Acquire and Maintain Application Software	
AI2.1 High-level Design	P.6 Software Development Lifecycle
AI2.2 Detailed Design	P.6 Software Development Lifecycle
AI2.3 Application Control and Auditability	P.6 Software Development Lifecycle
AI2.4 Application Security and Availability	P.6 Software Development Lifecycle
AI2.5 Configuration and Implementation of Acquired Application Software	F.2 Application Management
AI2.6 Major Upgrades to Existing Systems	P.6 Software Development Lifecycle
AI2.7 Development of Application Software	P.6 Software Development Lifecycle
AI2.8 Software Quality Assurance	P.25 Quality Management
AI2.9 Applications Requirements Management	P.6 Software Development Lifecycle
AI2.10 Application Software Maintenance	P.6 Software Development Lifecycle
AI3 Acquire and Maintain Technology Infrastructure	
AI3.1 Technological Infrastructure Acquisition Plan	F.3 Technical Management
AI3.2 Infrastructure Resource Protection and Availability	F.3 Technical Management
AI3.3 Infrastructure Maintenance	F.3 Technical Management
AI3.4 Feasibility Test Environment	P.20 Test Management F.3 Technical Management
AI4 Enable Operation and Use	
AI4.1 Planning for Operational Solutions	F.4 Operational Management F.2 Application Management F.3 Technical Management
AI4.2 Knowledge Transfer to Business Management	P.21 Knowledge Management
AI4.3 Knowledge Transfer to End Users	P.21 Knowledge Management

AI4.4 Knowledge Transfer to Operations and Support Staff	P.21 Knowledge Management
AI5 Procure IT Resources	
AI5.1 Procurement Control	P.15 Supplier Management
AI5.2 Supplier Contract Management	P.15 Supplier Management
AI5.3 Supplier Selection	P.15 Supplier Management
AI5.4 IT Resources Acquisition	P.15 Supplier Management
AI6 Manage Changes	
AI6.1 Change Standards and Procedures	P.18 Change Management
AI6.2 Impact Assessment, Prioritization and Authorization	P.18 Change Management
AI6.3 Emergency Changes	P.18 Change Management
AI6.4 Change Status Tracking and Reporting	P.18 Change Management
AI6.5 Change Closure and Documentation	P.18 Change Management
AI7 Install and Accredite Solutions and Changes	
AI7.1 Training	P.19 Release and Deployment Management
AI7.2 Test Plan	P.20 Test Management
AI7.3 Implementation Plan	P.19 Release and Deployment Management
AI7.4 Test Environment	P.20 Test Management
AI7.5 System and Data Conversion	P.19 Release and Deployment Management
AI7.6 Testing of Changes	P.20 Test Management
AI7.7 Final Acceptance Test	P.20 Test Management
AI7.8 Promotion to Production	P.19 Release and Deployment Management
AI7.9 Post-implementation Review	P.19 Release and Deployment Management
DS1 Define and Manage Service Levels	
DS1.1 Service Level Management Framework	P.8 Service Level Management
DS1.2 Definition of Services	Service Catalogue Management
DS1.3 Service Level Agreements	P.8 Service Level Management
DS1.4 Operating Level Agreements	P.8 Service Level Management
DS1.5 Monitoring and Reporting of Service Level Achievements	P.8 Service Level Management
DS1.6 Review of Service Level Agreements and Contracts	P.8 Service Level Management
DS2 Manage Third-party Services	
DS2.1 Identification of All Supplier Relationships	P.15 Supplier Management
DS2.2 Supplier Relationship Management	P.15 Supplier Management

DS2.3 Supplier Risk Management	P.15 Supplier Management
DS2.4 Supplier Performance Monitoring	P.15 Supplier Management
DS3 Manage Performance and Capacity	
DS3.1 Performance and Capacity Planning	P.10 Capacity Management
DS3.2 Current Performance and Capacity	P.10 Capacity Management P.13 Event Management
DS3.3 Future Performance and Capacity	P.10 Capacity Management
DS3.4 IT Resources Availability	P.12 Availability Management
DS3.5 Monitoring and Reporting	P.10 Capacity Management P.12 Availability Management
DS4 Ensure Continuous Service	
DS4.1 IT Continuity Framework	P.11 Continuity Management
DS4.2 IT Continuity Plans	P.11 Continuity Management
DS4.3 Critical IT Resources	P.11 Continuity Management
DS4.4 Maintenance of the IT Continuity Plan	P.11 Continuity Management
DS4.5 Testing of the IT Continuity Plan	P.11 Continuity Management
DS4.6 IT Continuity Plan Training	P.11 Continuity Management
DS4.7 Distribution of the IT Continuity Plan	P.11 Continuity Management
DS4.8 IT Services Recovery and Resumption	P.11 Continuity Management
DS4.9 Offsite Backup Storage	P.11 Continuity Management P.5 Risk Management
DS4.10 Post-resumption Review	P.11 Continuity Management
DS5 Ensure Systems Security	
DS5.1 Management of IT Security	P.14 Information Security Management
DS5.2 IT Security Plan	P.14 Information Security Management
DS5.3 Identity Management	P.14 Information Security Management P.22 Request Management
DS5.4 User Account Management	P.14 Information Security Management P.22 Request Management
DS5.5 Security Testing, Surveillance and Monitoring	P.14 Information Security Management
DS5.6 Security Incident Definition	P.14 Information Security Management
DS5.7 Protection of Security Technology	P.14 Information Security Management
DS5.8 Cryptographic Key Management	P.14 Information Security Management

DS5.9 Malicious Software Prevention, Detection and Correction	P.14 Information Security Management
DS5.10 Network Security	P.14 Information Security Management
DS5.11 Exchange of Sensitive Data	P.14 Information Security Management
DS6 Identify and Allocate Costs	
DS6.1 Definition of Services	P.7 Catalogue Management P.3 Financial Management
DS6.2 IT Accounting	P.3 Financial Management
DS6.3 Cost Modelling and Charging	P.3 Financial Management
DS6.4 Cost Model Maintenance	P.3 Financial Management
DS7 Educate and Train Users	
DS7.1 Identification of Education and Training Needs	P.8 Service Level Management P.16 Human Resources Management
DS7.2 Delivery of Training and Education	P.8 Service Level Management P.16 Human Resources Management
DS7.3 Evaluation of Training Received	P.8 Service Level Management P.16 Human Resources Management
DS8 Manage Service Desk and Incidents	
DS8.1 Service Desk	F.1 Service Desk
DS8.2 Registration of Customer Queries	F.1 Service Desk P.23 Incident Management
DS8.3 Incident Escalation	P.23 Incident Management
DS8.4 Incident Closure	P.23 Incident Management
DS8.5 Reporting and Trend Analysis	P.23 Incident Management F.1 Service Desk
DS9 Manage the Configuration	
DS9.1 Configuration Repository and Baseline	P.9 Configuration Management
DS9.2 Identification and Maintenance of Configuration Items	P.9 Configuration Management
DS9.3 Configuration Integrity Review	P.9 Configuration Management P.24 Problem Management P.23 Incident Management P.18 Change Management
DS10 Manage Problems	
DS10.1 Identification and Classification of Problems	P.24 Problem Management
DS10.2 Problem Tracking and Resolution	P.24 Problem Management

DS10.3 Problem Closure	P.24 Problem Management
DS10.4 Integration of Configuration, Incident and Problem Management	P.24 Problem Management P.9 Configuration Management P.23 Incident Management P.24 Problem Management
DS11 Manage Data	
DS11.1 Business Requirements for Data Management	P.21 Knowledge Management
DS11.2 Storage and Retention Arrangements	P.21 Knowledge Management
DS11.3 Media Library Management System	P.21 Knowledge Management
DS11.4 Disposal	P.21 Knowledge Management
DS11.5 Backup and Restoration	P.21 Knowledge Management F.3 Technical Management IT Operation Management
DS11.6 Security Requirements for Data Management	P.5 Risk Management P.14 Information Security Management
DS12 Manage the Physical Environment	
DS12.1 Site Selection and Layout	F.4 Operation Management
DS12.2 Physical Security Measures	F.4 Operation Management
DS12.3 Physical Access	F.4 Operation Management
DS12.4 Protection Against Environmental Factors	F.4 Operation Management
DS12.5 Physical Facilities Management	F.4 Operation Management
DS13 Manage Operations	
DS13.1 Operations Procedures and Instructions	F.2 Application Management F.3 Technical Management F.4 Operation Management
DS13.2 Job Scheduling	F.4 Operation Management
DS13.3 IT Infrastructure Monitoring	P.13 Event Management
DS13.4 Sensitive Documents and Output Devices	F.4 Operation Management
DS13.5 Preventive Maintenance for Hardware	F.3 Technical Management
ME1 Monitor and Evaluate IT Performance	
ME1.1 Monitoring Approach	P.25 Quality Management Service Management
ME1.2 Definition and Collection of Monitoring Data	P.25 Quality Management Service Management
ME1.3 Monitoring Method	P.25 Quality Management Service Management

ME1.4 Performance Assessment	P.25 Quality Management Service Management
ME1.5 Board and Executive Reporting	P.25 Quality Management Service Management
ME1.6 Remedial Actions	P.25 Quality Management Service Management
ME2 Monitor and Evaluate Internal Control	
ME2.1 Monitoring of Internal Control Framework	P.25 Quality Management
ME2.2 Supervisory Review	P.25 Quality Management
ME2.3 Control Exceptions	P.25 Quality Management
ME2.4 Control Self-assessment	P.25 Quality Management
ME2.5 Assurance of Internal Control	P.25 Quality Management
ME2.6 Internal Control at Third Parties	P.25 Quality Management
ME2.7 Remedial Actions	P.25 Quality Management
ME3 Ensure Compliance With External Requirements	
ME3.1 Identification of External Legal, Regulatory and Contractual Compliance Requirements	P.25 Quality Management
ME3.2 Optimization of Response to External Requirements	P.25 Quality Management
ME3.3 Evaluation of Compliance With External Requirements	P.25 Quality Management
ME3.4 Positive Assurance of Compliance	P.25 Quality Management
ME3.5 Integrated Reporting	P.25 Quality Management
ME4 Provide IT Governance	
ME4.1 Establishment of an IT Governance Framework	Definition of IT Governance
ME4.2 Strategic Alignment	IT Governance Focus Areas
ME4.3 Value Delivery	IT Governance Focus Areas
ME4.4 Resource Management	IT Governance Focus Areas
ME4.5 Risk Management	IT Governance Focus Areas
ME4.6 Performance Measurement	IT Governance Focus Areas
ME4.7 Independent Assurance	P.25 Quality Management

APPENDIX M – Mapping ITIL v3 with Framework

SS 4.1 Define the market	P.1 IT Management P.7 Catalogue Management
SS 4.2 Develop the offerings	P.7 Catalogue Management P.2 Portfolio Management
SS 4.4 Prepare for execution	P.1 IT Management P.2 Portfolio Management
SS 5.1 Financial management	P.3 Financial Management
SS 5.1.3.4 Business Impact Analysis	P.11 Continuity Management
SS 5.2 Return on investment	P.3 Financial Management
SS 5.3 Service portfolio management	P.2 Portfolio Management
SS 5.4 Service portfolio management methods	P.2 Portfolio Management
SS 5.5 Demand management	P.22 Request Management P.8 Service Level Management
SS 6.1 Organizational development	P.1 IT Management
SS 6.2 Organizational departmentalization	P.1 IT Management
SS 6.3 Organizational design	P.1 IT Management
SS 6.4 Organizational culture	P.1 IT Management
SS 6.5 Sourcing strategy	P.15 Supplier Management
SS 7.5 Strategy and improvement	P.12 Availability Management
SS 8.1 Service automation	F.2 Application Management P.6 Software Development Lifecycle
SS 8.3 Tools for service strategy (focused on DS1)	Tools in processes
SS 9.1 Complexity	P.1 IT Management
SS 9.2 Co-ordination and control	P.1 IT Management
SS 9.3 Preserving value	P.1 IT Management
SS 9.4 Effectiveness in measurement	P.25 Quality Management
SS 9.5 Risks	P.5 Risk Management
SD 3.3 Identifying service requirements	F.2 Application Management F.3 Technical Management

SD 3.4 Identifying and documenting business requirements and drivers	P.17 Project Management P.6 Software Development Lifecycle F.2 Application Management F.3 Technical Management
SD 3.5 Design activities	Inputs for all Service processes Outputs from all Service processes
SD 3.6 Design aspects	P.3 Financial Management Service Management P.2 Portfolio Management
SD 3.6.1 Designing service solutions	P.6 Software Development Lifecycle F.2 Application Management
SD 3.6.2 Designing supporting systems, especially the service portfolio	P.2 Portfolio Management
SD 3.6.3 Designing technology architectures	P.4 Corporate Architecture F.2 Application Management Technological Management P.21 Knowledge Management P.1 IT Management
SD 3.6.4 Designing processes	P.1 IT Management
SD 3.6.5 Design of measurement systems and metrics	Metrics for all processes P.25 Quality Management
SD 3.7.1 Evaluation of alternative solutions	P.15 Supplier Management F.2 Application Management
SD 3.7.2 Procurement of the preferred solution	P.15 Supplier Management
SD 3.7.3 Develop the service solution (development is just mentioned)	P.6 Software Development Lifecycle
SD 3.8 Design constraints	F.2 Application Management F.3 Technical Management
SD 3.11 Service design models	P.1 IT Management
SD 4.x.1 Purpose/goal/objective	Purpose and Goal for all processes
SD 4.1 Service catalogue management	P.7 Catalogue Management
SD 4.2 Service level management	P.8 Service Level Management
SD 4.3 Capacity management	P.10 Capacity Management
SD 4.4 Availability management	P.12 Availability Management
SD 4.5 IT service continuity management	P.11 Continuity Management
SD 4.6 Information security management	P.14 Information Security Management
SD 4.7 Supplier management	P.15 Supplier Management

SD 5.1 Requirements engineering	P.6 Software Development Lifecycle
SD 5.2 Data and information management	P.21 Knowledge Management
SD 5.3 Application management	P.6 Software Development Lifecycle
SD 6.1 Functional roles analysis	Roles in Processes
SD 6.2 Activity analysis	Roles in Processes
SD 6.3 Skills and attributes	Skills Inventory P.1 IT Management
SD 6.4 Roles and responsibilities	Roles in Processes
SD 7 Technology considerations	Tools in processes
SD 8.1 Business impact analysis (not in detail)	P.11 Continuity Management
SD 8.2 Service level requirements	P.8 Service Level Management
SD 8.3 Risks to the services and processes	P.5 Risk Management
SD 8.5 Measurement of service design	P.25 Quality Management
ST 4.2 Change management	P.18 Change Management
ST 4.2.6.8 Change advisory board	Roles in Processes
ST 4.2.6.9 Emergency changes	Roles in Processes
ST 4.2.7 Triggers, input and output, and inter-process interfaces	P.18 Change Management
ST 4.3 Service asset and configuration management	P.9 Configuration Management
ST 4.4 Release and deployment management	P.19 Release and Deployment Management
ST 4.4.5.1 Planning	P.19 Release and Deployment Management P.20 Test Management
ST 4.4.5.2 Preparation for build, test and deployment	P.19 Release and Deployment Management
ST 4.4.5.3 Build and test	P.20 Test Management
ST 4.4.5.4 Service testing and pilots	P.20 Test Management
ST 4.4.5.5 Plan and prepare for deployment	P.19 Release and Deployment Management
ST 4.4.5.6 Perform transfer, deployment and retirement	P.19 Release and Deployment Management
ST 4.4.5.7 Verify deployment	P.19 Release and Deployment Management
ST 4.4.5.8 Early life support	P.19 Release and Deployment Management

ST 4.4.5.9 Review and close a deployment	P.19 Release and Deployment Management
ST 4.4.5.10 Review and close service transition	P.19 Release and Deployment Management
ST 4.5 Service validation and testing (ITIL is not focused just on service transition, but on ongoing test of the service.)	P.20 Test Management
ST 4.6 Evaluation	P.19 Release and Deployment Management
ST 4.7 Knowledge management	P.21 Knowledge Management
ST 5 Service transition common operation activities	P.1 IT Management P.18 Change Management
ST 5.1 Managing communications and commitment	P.1 IT Management
ST 5.2 Managing organization and stakeholder change	P.18 Change Management
ST 6.1 Generic roles	Roles
ST 6.2 Organizational context for transitioning a service	P.1 IT Management
ST 6.3 Organization models to support service transition	P.1 IT Management Roles in Processes
ST 7 Technology considerations	Tools in processes
ST 8 Implementing service transition	P.17 Project Management P.1 IT Management
SO 3 Service operation principles	P.1 IT Management
SO 3.7 Documentation	F.2 Application Management F.4 Operational Management F.3 Technical Management
SO 4 Service operation processes	Service Operation Processes
SO 4.1 Event management	P.13 Event Management
SO 4.2 Incident management	P.23 Incident Management
SO 4.3 Request fulfillment	P.22 Request Management
SO 4.4 Problem management	P.24 Problem Management
SO 4.5 Access management	P.14 Information Security Management P.22 Request Management
SO 4.6.1 Change management (as operational activities)	P.18 Change Management
SO 4.6.2 Configuration management (as operational activities)	P.9 Configuration Management

SO 4.6.3 Release and deployment management (as operational activities)	P.19 Release and Deployment Management
SO 4.6.4 Capacity management (as operational activities)	P.10 Capacity Management
SO 4.6.5 Availability management (as operational activities)	P.12 Availability Management
SO 4.6.6 Knowledge management (as operational activities)	P.21 Knowledge Management
SO 4.6.7 Financial management for IT services (as operational activities)	P.3 Financial Management
SO 4.6.8 IT Service continuity management	P.11 Continuity Management
SO 5.1 Monitoring and control	P.25 Quality Management F.4 Operational Management
SO 5.2 IT operations	F.4 Operational Management
SO 5.2.1 Console management/operations bridge	P.13 Event Management
SO 5.2.2 Job scheduling	F.4 Operational Management
SO 5.2.3 Backup and restore	F.4 Operational Management P.21 Knowledge Management
SO 5.2.4 Print and output	F.4 Operational Management
SO 5.3 Mainframe management	F.4 Operational Management
SO 5.4 Server management and support	F.4 Operational Management IT Infrastructure Management P.14 Information Security Management
SO 5.5 Network management	F.3 Technical Management
SO 5.6 Storage and archive	F.4 Operational Management
SO 5.7 Database administration	F.3 Technical Management
SO 5.8 Directory services management	F.3 Technical Management
SO 5.9 Desktop support	F.3 Technical Management
SO 5.10 Middleware management	F.3 Technical Management
SO 5.11 Internet/web management	F.3 Technical Management
SO 5.12 Facilities and data centre management	F.4 Operational Management
SO 5.13 Information security management and service operation (vague)	Security Management P.16 Human Resources Management
SO 6.1 Functions	F.1 Service Desk F.3 Technical Management F.4 Operational Management P.6 Software Development

	Lifecycle
SO 6.2 Service desk	F.1 Service Desk
SO 6.3 Technical management	Tools F.3 Technical Management
SO 6.4 IT operations management	F.4 Operational Management
SO 6.5 Application management	F.2 Application Management P.6 Software Development Lifecycle
SO 6.6 Service operation roles and responsibilities	Roles and Responsibilities of processes
SO 6.7 Service operation organization structures	P.1 IT Management
SO 7 Technology considerations (especially for licensing, mentioned in SO 7.1.4)	Tools in processes
SO 8 Implementing service operation	P.1 IT Management
CSI Introduction	P.25 Quality Management
CSI 3 CSI principles	P.25 Quality Management
CSI 4.2 Service reporting	P.25 Quality Management
CSI 4.3 Service measurement	P.25 Quality Management
SO 3.7 Documentation	F.2 Application Management F.4 Operational Management F.3 Technical Management
CSI 4.5 Business questions for CSI	P.25 Quality Management
CSI 4.6 Service level management	P.8 Service Level Management
CSI 5.1 Methods and techniques	P.25 Quality Management
CSI 5.2 Assessments	P.25 Quality Management
CSI 5.3 Benchmarking	P.25 Quality Management
CSI 5.4 Measuring and reporting frameworks	P.1 IT Management
CSI 5.5 The Deming Cycle	P.25 Quality Management
CSI 5.6.1 Availability management	P.12 Availability Management
CSI 5.6.2 Capacity management	P.10 Capacity Management
CSI 5.6.3 IT service continuity management	P.11 Continuity Management P.5 Risk Management P.14 Information Security Management
CSI 5.6.4 Problem management	P.24 Problem Management

CSI 5.6.5 Change, release and deployment management	P.18 Change Management
CSI 5.6.6 Knowledge management	P.21 Knowledge Management
CSI 6 Organising for continual service improvement	Roles in processes
CSI 7 Technology considerations	Tools in processes

APPENDIX N – Qualitative Research Questions

QUESTION 1: What do you think about the necessity of information technologies for private or government organizations? If it is necessary, how much is it important and why ?

QUESTION 2: Are you implementing any IT governance framework / standard into your organization? If you implement any framework, is it satisfying you?

QUESTION 3: Do you have any idea what this framework or standard is selected? Can you explain?

COBIT

QUESTION 5: What do you think about the reason of difficulties in implementation of COBIT?

QUESTION 6: Do you think that COBIT has any deficiency or surplus?

QUESTION 7: Is RACI chart in COBIT is applicable?

ITIL




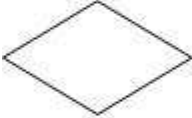



QUESTION 8: What do you think about the reason of difficulties in implementation of COBIT?

QUESTION 9: Do you think that COBIT has any deficiency or surplus?

QUESTION 10: Do you want a web site including IT processes prepared in Turkish?

QUESTION 11: Do you want to say anything else?

APPENDIX O – Figure Explanations

Figures	Explanations
	Shows that the beginning and ending of process
	Shows the processes steps
	Shows the predefined process
	Shows the decision
	Shows the output-document
	Shows the electronic output
	Show the roles