CANKAYA UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
DEPARTMENT OF MANAGEMENT

MASTER THESIS

THE COMPARISON OF INFORMATION SECURITY STANDARDS BY USING ANALYTIC HIERARCHY PROCESS

NURCAN TATAR

FEBRUARY 2015

Title of the Thesis : **The Comparison of Information Security Standards by Using Analytic Hierarchy Process**

Submitted by : **Nurcan TATAR**

Approval of the Graduate School of Social Sciences, Çankaya University

Mehmet yazıcı

Prof. Dr. Mehmet YAZICI
Director

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

Mete Doğanay

Prof. Dr. Mehmet Mete DOĞANAY
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.

Asst. Prof. Ayşegül TAŞ
Supervisor

Examination Date: 03 February 2015

Examining Committee Members:

Asst. Prof. Mine ÖMÜRGÖNÜLŞEN (Hacettepe Univ.) Mine

Assoc. Prof. Rabia Arzu KALEMCİ (Çankaya Univ.) ---------------------------------

Asst. Prof. Ayşegül TAŞ (Çankaya Univ.) ---------------------------------

THESIS STATEMENT

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 : Nurcan TATAR

Signature :

Date : 03.02.2015

ABSTRACT

THE COMPARISON OF INFORMATION SECURITY STANDARDS BY USING ANALYTIC HIERARCHY PROCESS

TATAR, Nurcan
Master Thesis
Graduate School of Social Sciences, MBA
Supervisor: Asst. Prof. Ayşegül TAŞ

February 2015, 92 pages

Information security has gained a great importance in today's world. Information security and information security standards have taken its place among popular research areas. The purpose of this study is to select the best information security standard by using Analytic Hierarchy Process technique. The problem is modeled by multi-criteria decision making. Multi-criteria decision making is a method that is used for complex problems. In this study, first of all, information security standards are selected according to their worldwide popularity and explained in detail to give an idea. Then, common criteria of the standards are determined. Finally, the alternatives are evaluated with the help of Expert Choice Package regarding determined criteria. As a result of this study, it is seen that even though COBIT has superiority compare with ISO 27001 and ITIL based on specific criteria, when comparing ISO 27000 series with COBIT and ITIL, this time ISO 27000 series has gained superiority over COBIT and ITIL. None of these standards can promise hundred percent success in providing information security when applied singly. Therefore, a road map has been prepared to increase the effectiveness of information security system by combining these standards.

Key Words: MCDM, AHP, Information Security, COBIT, ITIL, ISO/IEC 27001.

ÖZ

BİLGİ GÜVENLİĞİ STANDARTLARININ ANALİTİK HİYERARŞİ PROSESİ YAKLAŞIMI İLE KARŞILAŞTIRILMASI

TATAR, Nurcan
Yüksek lisans Tezi
Sosyal Bilimler Enstitüsü, İşletme Yönetimi
Tez Yöneticisi: Yrd. Doç. Dr. Ayşegül TAŞ

Şubat 2015, 92 sayfa

Günümüzde bilgi güvenliği büyük bir önem kazanmıştır. Bilgi güvenliği ve bilgi güvenliği standartları konuları yaygın araştırma konuları arasında yerlerini almıştır. Bu tezin amacı, Analitik Hiyerarşi Metodunu kullanarak en iyi bilgi güvenliği standardını seçmektir. Araştırmada yer alan problem, çok ölçütlü karar verme yöntemine göre şekillendirilmiştir. Çok ölçütlü karar verme karmaşık problemlerin olduğu durumlarda kullanılan bir metottur. Yapılan çalışmada, öncelikli olarak, bilgi güvenliği standartları kullanım yaygınlıklarına göre seçilmiş olup, seçilmiş olan standartlar fikir vermesi açısından detaylı bir şekilde anlatılmıştır. Daha sonra, standartlarda yer alan ortak kriterler belirlenmiştir. Son olarak, alternatifler Expert Choice Programı yardımı ile değerlendirilmiştir. Çalışmanın sonucunda, seçilen kriterlere göre COBIT her ne kadar ISO 27001 ve ITIL'a göre üstünlüğe sahip olsa da, ISO27000 serisinin COBIT ve ITIL ile karşılaştırıldığında bu kez ISO 27000 serisinin üstünlük kazandığı görülmüştür. Standartların hiçbiri tek başına kullanıldığında bilgi güvenliğinde yüzde yüz başarı temin etmemektedir. Bu sebeple, bilgi güvenliği etkinliğini arttırmak amacıyla söz konusu standartları birleştiren bir yol haritası hazırlanmıştır.

Anahtar Kelimeler: ÇÖKV, AHP, Bilgi Güvenliği, COBIT, ITIL, ISO/IEC 27001.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my advisor Asst. Prof. Ayşegül Taş for her continuous support during the preparation of my research, her for patience, motivation and immense knowledge.

Besides my advisor, I would like to thank Auditor Aydın Şeker from İlbank INC. Committee of Inspection. Last but not the least; I would like to thank my family for the support they provided me through my entire life.

Ankara; February, 2015 **Nurcan TATAR**

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

AI	: Acquire and Implement
AHP	: Analytic Hierarchy Process
CCTA	: Central Computer and Telecommunications Agency
CERT	: Computer Emergency Response Team
CI	: Consistency Index
CNSS	: Committee on National Security Systems
COBIT	: Control Objectives for Information and Related Technology
CR	: Consistency Ratio
CSIP	: Project Management and a Continuous Service Improvement Program
DS	: Deliver and Support
IEC	: International Electrotechnical Commission
ISACA	: Information Systems Audit and Control Association
ISMS	: Information Security Management System
ISO	: International Organization for Standardization
IT	: Information Technology
ITIL	: Information Technology Infrastructure Library
ITSM	: Information Technology Service Management
JTC	: Joint Technical Committee
MCDM	: Multi-criteria Decision Making
ME	: Monitor and Evaluate
OGC	: Office of Government Commerce
PMF	: Appropriate Goal Setting Through a Process Maturity Framework
PO	: Plan and Organize
SACM	: Service Asset and Configuration Management
SPM	: Service Portfolio Management

CHAPTER I

INTRODUCTION

Information has a vital role in each part of life. It helps people to make decisions in different situations. Information is a fundamental asset for organizations. It is as important as other products that an organization serves. Because, it is not possible to have all information, the exchange of data is essential. Thus, information has to be protected properly and continuously against any external or internal threat. Information security is achieved by protecting the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission. Information security is very important because it ensures the continuous functioning of the organization and protection of data created, collected and utilized.

In order to be able to explain what decision making is, decision should be defined first. Decision is the choice made within the framework of various cognitive actions. While making decisions, the purpose is to get satisfying results. Decision making is simply defined as the selection of the most appropriate alternatives. It is based on at least one purpose. Decisions are made between several possible alternatives. At the end of the process, people reach a final choice. Decision making has a certain starting point and composed by several steps. In order to make good decisions, it is vital to know the process that should be followed. There are many factors that affect decision making process such as purpose(s), options, the results of alternatives and the perception of decision maker.

Information security is the protection of information and its censorious components. The security of information has a great importance for organizations. Especially in last years, many studies have been conducted in the area of information security. This research is conducted in order to compare the standards and best practices from the point of information security aspect. Thus, most widely used standards and best practices are examined. COBIT, ITIL and ISO 27001 are selected. COBIT is an IT governance framework and it helps managers to bridge the gap between control requirements, business risks and technical and security issues. In COBIT, there are a set of control objectives and practices which define what to do in order to establish and maintain a successful Information Technology performance. There are several processes and in each of the process a number of control objectives take place. The domains of the standard are Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS) and Monitor and Evaluate (ME). ITIL is an information library which is composed by best applications, practices and experiences. It encourages quality computing services in the area of information technology. ITIL contains a set of processes. The roles and responsibilities of all parties are clear and well-defined. Therefore, everyone in the organization is aware of what they are expected to do. ISO 27001 is the requirement for planning, implementation, operation and continuous monitoring and development of a process-oriented information security management system. It includes the requirements for the evaluation and treatment of information security risks tailored to the needs of the organization. The requirements of the standard are generic and can be applied in all organizations easily.

Information Technology is increasing the effectiveness of organizations. It is possible to have more competitive advantage with a successful Information Technology system. Governmental Institutions are also paying more attention to information security by the legal obligations they have established. With these obligations, it became a must to have smooth security systems. Unfortunately it is not possible to say that they are understood and implemented properly by everyone. For instance, in the banking sector, some of the players know what they are expected to do but they don’t know how to design things and improve themselves from the point of Information Technology security.

Several studies have been done in the literature. According to Susanto et al. (2011), there are big five which are ISO 27001, BS7799, PCIDSS, COBIT and ITIL. It is seen in the research that ISO is more implemented smoothly, stakeholders can recognize it easily and the standard has appropriate platform in an organization deal with, than four other security standards. According to Mataracıoğlu and Ozkan (2011), ISO 27001 describes the information security duties in a more comprehensive manner than COBIT does. Nevertheless, it is indicated that ISO 27001 and COBIT have to work together in providing the information security governance. Sheikhpour and Modiri (2012) suggests that integration of ISO 27001 into ITIL service management processes enables an organization to lower the overall costs and manage the risks. According to Pena et. al. (2013), ITIL and COBIT are complementary rather than competing. It is specified that COBIT can guide organizations in what should be covered in processes and procedures whereas ITIL guides on how the processes or procedures should be designed. Gehrmann (2012) suggests that ITIL methodology should be used to define the strategies, concepts and processes related to IT management. COBIT should be used to evaluate the critical success factors, metrics, indicators and audits whereas ISO/IEC 27002 standard should guide the management of IT in relation to issues of IT security.

There are several studies about information security standards in the literature. Most of the studies briefly suggest the integration of different standards but they don’t indicate how to do it. The main purpose of this study is to investigate the ways to increase the effectiveness of information security by comparing and then combining the most widely used international standards. As distinct to other studies, Analytic Hierarchy Process (AHP) method is implemented to determine the best information security standard based on selected criteria. In this study, literature study has been performed in order to give detailed information on information security, information security standards and decision making process. In order to decide which standard is the best in the field of information security, pair-wise comparisons are done. The opinion of experts and users are taken by making interview questionnaires with them.

This study is composed by six parts. In the first part, an introduction is made to give an idea about the research. In the second part, the concept of information and information security are analyzed. Threats on information security and incidents that may occur are defined.

In the third part of the study, most used information security standards and best practices which are Control Objectives for Information and Related Technology, The Information Technology Infrastructure Library and ISO 27001 are addressed from the point of their content and implementations.

In the fourth part, decision making process is addressed. The concept of decision and decision making are defined. The Analytic Hierarchy Process method is defined as the theory of evaluation by making pair-wise comparisons and relies on the judgments of the decision maker. It is one of the best methods in multi-criteria decision problems and applied in complex situations. The method, its advantages and disadvantages, steps and applied software package are addressed in this part.

In the fifth part, information security standards and best practices are compared based on identified criteria. The purpose and content of the research, methodology, and data collection, steps of the implementation and pair-wise comparisons and its results are demonstrated.

In the last part of the study, the results of the research is analyzed and interpreted. The information security standards that are selected for the study are evaluated from the point of their effectiveness.

CHAPTER II

2. INFORMATION AND INFORMATION SECURITY

In this chapter, the concept of information and information security are analyzed. The confidentiality, integrity and availability components of the CIA Triad are addressed. Threats on information security and incidents that may occur are defined.

2.1. THE CONCEPT OF INFORMATION AND SECURITY

There are many definitions of information. Information is defined as data recorded, classified, organized, related or interpreted within context to convey meaning (Duffy and Assad, 1980, pg.13). Another definition is that information is any physical form of representation or surrogate of knowledge or of a particular thought used for communication (Farradane, 1979, pg. 13). It is possible to define information simply as data endowed with relevance and purpose.

Information helps us to reduce uncertainty and make decisions in different situations. In other words, information is used in making decisions and taking actions based on the decisions made. Information has a vital role in each part of life. For the reason that it is not possible to hold all the information, exchange of data between different departments, institutions, people or technologies is needed. Unfortunately, sharing of information increases the risks that an organization faces. Because of this fact, the person who shares information has to take actions to protect it against any internal or external threat.

Security is simply defined as “the state of being protected or safe from harm-freedom from danger” (http://www.merriam-webster.com/dictionary/security). A successful organization should have the following multiple layers of security (Withman and Mattord, 2011, pg. 8):

- Physical security should be provided in order to protect physical items, objects or areas from unauthorized access or misuse by others.
- Personnel security should be provided in order to protect the individual or group of individuals who are authorized to access the organization and its operations.
- Operation security should be provided in order to protect the details of particular operation or series of activities.
- Communication security should be provided in order to protect communications media, technology and content.
- Network security should be provided in order to protect networking components, connections and contents.
- Information security should be provided in order to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission.

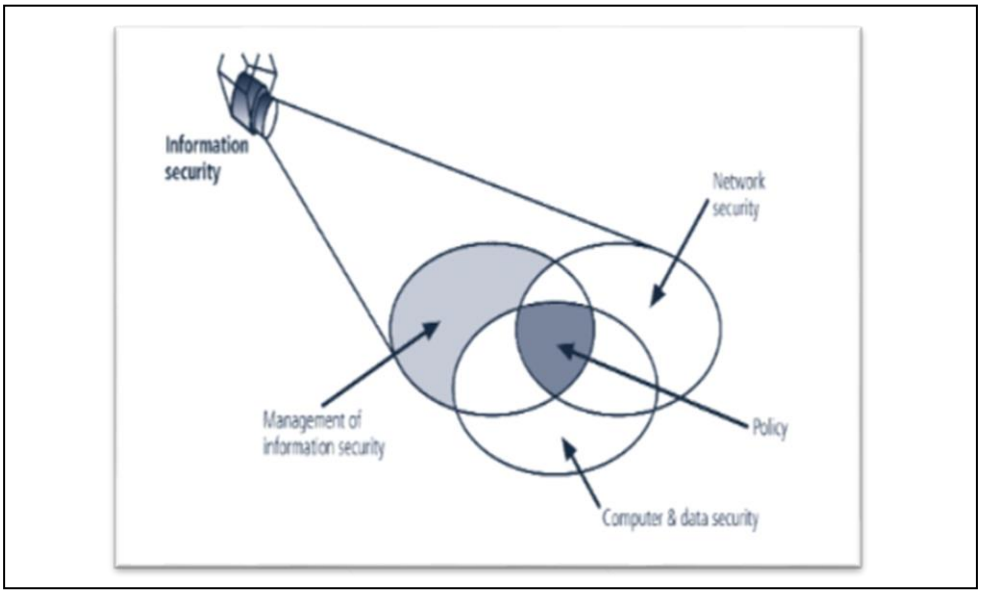


Figure 2.1: Components of Information Security
Source: Whitman and Mattord, Principles of Information Security, 2011

As seen in Figure 2.1, management of information security, network security, computer and data security are essential. Policy is in the intersection point and known as a written document which defines the ways to protect an organization's information technology.

2.2. THE CONCEPT OF INFORMATION SECURITY

Information is one of the most important assets that an organization holds. Because of this fact, it has to be protected properly and continuously by the organization. In order to provide the continuity of its operations, an organization should ensure the protection of information against any threats. The threats that an organization can be faced with may be either external or internal. Security is composed of two very important components: physical and electronical. For this reason, information must be protected both physically and electronically.

Information security is simply defined as the preservation of confidentiality, integrity and availability of information (ISO/IEC 27001 Standard). According to the Committee on National Security Systems (CNSS), information security is the protection of information and its censorious components, including the systems and hardware that use, store, and transfer the information.

In the case of unauthorized access, use or destruction of information or information systems, information security takes place in order to provide protection against any threat that can occur.

2.2.1. The Characteristics of Information System

Characteristics of information security have evolved in parallel with the technological advancements and as the points of view regarding the subject has gained a wider perception.

It is generally accepted that there are three characteristics of information systems: confidentiality, integrity and availability. It is known as the CIA Triad. Another name for it is information security triad.

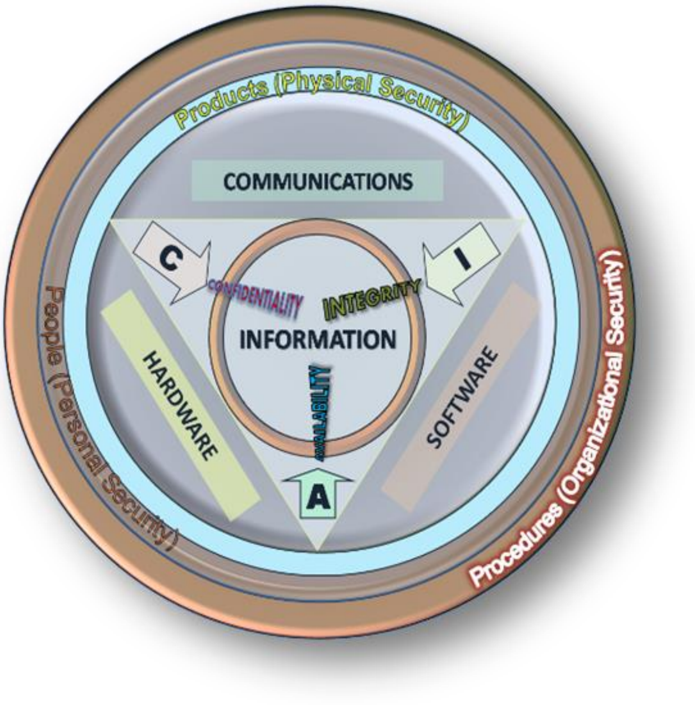

Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
AVAILABILITY
HARDWARE
SOFTWARE
A
People (Personal Security)
Procedures (Organizational Security)

Figure 2.2 **:** CIA Triad
Source : IT Security Review: Privacy, Protection, Access Control, Assurance and System Security

As seen in Figure 2.2, there are three information security attributes which are confidentiality, integrity and availability. An information system is formed by hardware, software and communications. The protection is done at three levels which are personal, physical and organizational.

An alternative model was developed by Donn Parker in 1998 which adds additional attributes to the classic structure of the CIA Triad. The name of the model is Parkerian Hexad. In the Parkerian Hexad model, there are six elements of information security which means that three more than the CIA Triad.

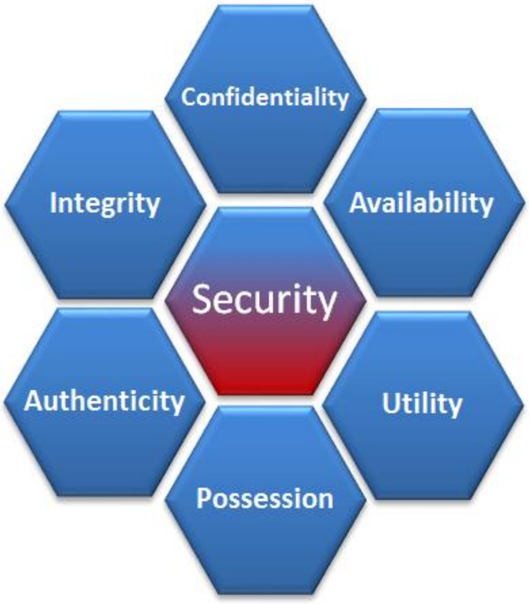


Figure 2.3 : Parkerian Hexad Model
Source : http://www.writeopinions.com/parkerian-hexad

The Figure 2.3 shows the attributes which take part in the Parkerian Hexad Model. According to this model, authenticity, utility and possession elements are added to the CIA Triad.

2.2.1.1. Confidentiality

Confidentiality is the element concerning the information that is available and accessible to only who are authorized within the scope of privacy, which ensures information only can only be controlled, collected, or stored by only related people.

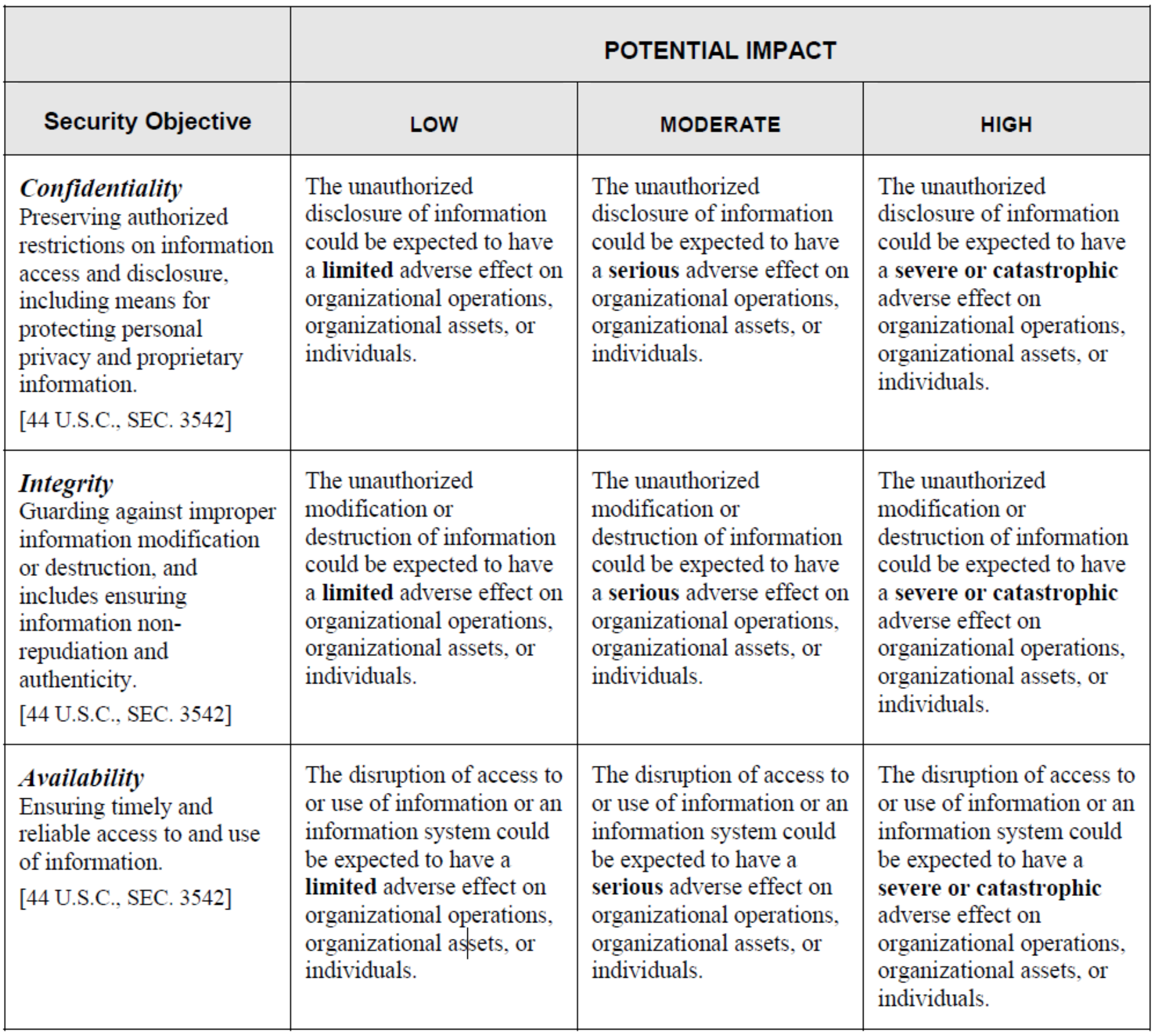
2.2.1.2. Integrity

Integrity is about taking necessary measurements against the incorrect modification, distortion or termination of information. The element of integrity can be mentioned on both data and system levels. While the former is in the scale of information and programs, the latter is about a system's functioning properly in line with its purposed design free from unauthorized access and manipulation.

2.2.1.3. Availability

The availability element is concerned about assuring the convenient access both to the system and the information it contains.

Table 2.1: Potential Impact Definitions for Security Objectives



	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Source: Standards for Security Categorization of Federal Information and Information Systems, 2004

Table 2.1 shows the potential impact of confidentiality, integrity, and availability on the base of the CIA Triad. They may have limited, serious or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

2.2.1.4 Authenticity

Authenticity comprehends the verification and validation of information creation and transmission together with user and data source identification.

2.2.1.5 Possession or Control

Possession or control describes the possibility, not the actual event of security breach, of unauthorized access (the loss of control) and information theft (the loss of possession) any time.

2.2.1.6 Utility

This element of the model focuses on the utilization problems of information at hand due to substitution difficulties in the form of data. Examples for this element can be given as follows (Baars et. al., 2010, pg.14):

- *"Suppose someone encrypted data on disk to prevent unauthorized access or undetected modifications – and then lost the decryption key: that would be a breach of utility. The data would be confidential, controlled, integral, authentic, and available – they just wouldn't be useful in that form.*
- *Conversion of salary data from one currency into an inappropriate currency would be a breach of utility, as would the storage of data in a format inappropriate for a specific computer architecture; e.g., EBCDIC instead of ASCII or 9-track magnetic tape instead of DVD-ROM."*

2.2.2. Information Security Incident

Information security is provided by the implementation of developed policies, procedures, programs, software and hardware functions. According to ISO/IEC 27035: 2011 Standard, incidents occur when controls are not reliable and effective enough. In order to manage security incidents, detective and corrective controls are implemented by the organization. An information security incident management policy should be planned and prepared. The events which turn to incidents should be recorded and reported regularly. Based on the reports, an assessment is done and decisions are made. After analyzing the responses, lessons learned should be documented from the results of the experienced incidents (ISO/IEC 27035:2011 Standard).

2.2.3. The Need for Information Security Based on Threats

Organizations put more emphasis on information security today. As a result, awareness of information security needs is increasing day by day. Studies in this area have been taking their place in history.

Information security is needed in order to provide the continuity of the operations an organization performs and to decrease the defects while operating. It is also essential to protect information against any internal or external threats. Information can exist in several forms. Regardless of the form it has, information should be protected properly by the organization. In such a manner, the need for information security can be derived from the functions of information security which are enumerated as follows:

- Ensuring the continuous functioning of the organization
- Facilitating convenient operational steps within the organizational body
- Protection of the data created, collected and utilized by the organization and any technological assets.

The functions mentioned above play a vital role in addressing the information security concerns that are derived from the identifications of threats listed below (http://www.utica.edu/faculty_staff/qma/needforsecurity.pdf):

- Human factor: Threats in this category are caused by insufficiently trained or inexperienced personnel and accidentally done without any bad intent. Such mistakes can lead to unrestricted access, deletion and modification classified data. Human factor is accepted as the most critical factor in information security.
- Disclosure of owned intellectual properties including software, trade secrets, copyrights, trademarks and patents
- Intended activities to cause a security breach such as unauthorized access, illegal data collection, data theft / destruction / corruption
- Information leakage: It occurs when unauthorized parties hold the information.
- Software attacks: Databases are kept on electronic platforms are targeted by software attacks. They include viruses, worms, Trojan horses, back doors,

denial of service and password related attacks, spoofing, spyware, spam, man-in-the-middle, buffer-overflow, logic-bomb, timing attack, sniffer and social engineering.

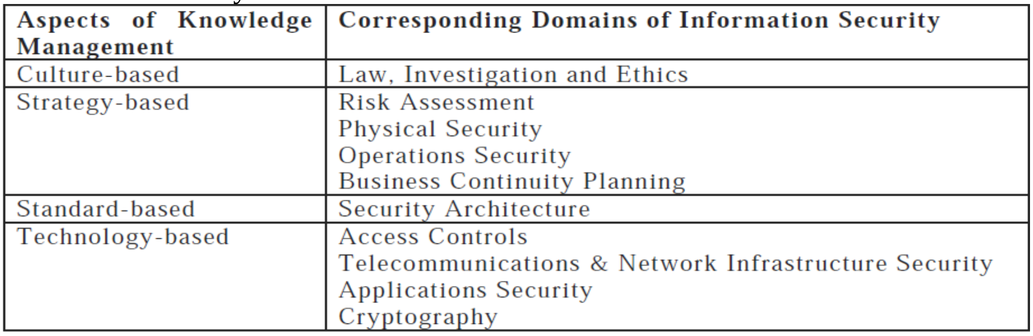
- Natural disasters that cause damage to data storage facilities, information access and transmission infrastructure. Against such unforeseen events data and system backups together with recovery procedures and contingency plans must be prepared and applied to ensure the continuity of operations within the organization.
- Insufficiencies or malfunctioning of supporting systems such as loss of internet, communication and utility services together with power irregularities, can cause serious security breaches in organizations even if they last only momentarily.
- Failure of office equipment: Hardware and software problems can suspend information availability temporarily or terminally.
- Outdated technological infrastructure: This kind of threat can be the fundamental reason of all the threats, except natural disasters, mentioned above.

2.3. AREAS OF INFORMATION SECURITY

Information security concepts can be analyzed in 10 areas, falling into four aspects of knowledge management. These areas of are listed below (Hansche, Berti, and Hare, 2003):

- Law, Investigation and Ethics
- Security Architecture
- Telecommunications & Network Infrastructure Security
- Access Controls
- Applications Security
- Cryptography
- Business Continuity Planning
- Operations Security
- Physical Security
- Information Security Management

Table 2.2: Conceptual Map of Knowledge Management Aspects and Domains of Information Security



Aspects of Knowledge Management	Corresponding Domains of Information Security
Culture-based	Law, Investigation and Ethics
Strategy-based	Risk Assessment Physical Security Operations Security Business Continuity Planning
Standard-based	Security Architecture
Technology-based	Access Controls Telecommunications & Network Infrastructure Security Applications Security Cryptography

Source: Security-based Knowledge Management, 2005.

As seen in Table 2.2, information security areas are categorized in four aspects of knowledge management which are culture-based, strategy-based, standard-based and technology-based (Ho and Wang, 2005, pgs. 3402-3403).

2.3.1. Culture-Based Aspect

Determining learning and sharing as the landmarks in an organization, culture based aspect focuses on leakage or inappropriate usage of information illegally in the process of intra-organizational sharing. Such vulnerability raises the concerns regarding the policies, monitoring, and authorization confirmation to manage the flow of information in the body of an organization.

2.3.2. Strategy-Based Aspect

Strategy-based aspect approaches the information handling practices of organizations, which can be grouped as collecting, processing, and storage, and dividing that whole process into phases (Green, Hurley, & Shaw, 2004). So, for each phase, a strategy appropriate for the sub-practices of the whole process can be determined in accordance with the nature of information.

The first phase includes the analysis and the assessment of potential risks, the level of exposures and the likelihood of attacks so that convenient physical and operational practices and measurements are taken before the collection of data is determined. The second phase includes overseeing the application and functioning of the methods decided in the first stage once the data is generated, stored, and processed and the information has started to be transmitted amongst the departments.

This phase commonly hosts strategies regarding monitoring, inspecting and reporting. The third stage includes strategies regarding the recovery and continuity plans in case of an occurrence of an incident or fatal security breach.

2.3.3. Content-Based Aspect

Content-based aspect focuses on the way the information content is gathered or kept, which is related to the security architecture. This aspect comprehends the international standards applied within the system (i.e. hardware, firmware, and software) of an organization to evaluate and compare the security levels.

2.3.4. Technology-Based aspect

Security concerns regarding the transformation of data into processed information constitute the back bone of this aspect. To illustrate, raw data is refined through some steps including data mining, storing, recording a backup, then analysis of such data with intelligent systems, and finally of the transmission of refined data within the organization via distribution intermediaries (networks or other storage mediums).

In today’s time, together with the data being collected, preserved, analyzed and transmitted digitally rather than physically, the measures taken for security have shifted accordingly. In other words, thanks to the technological advancements simultaneously happening as the form of information changed, it has brought about inevitable innovation to the way it is managed by organizations in terms of equipment, systems and policies.

In the next chapter, information, information security and its standards will be explained in detail.

CHAPTER III

3. INFORMATION SECURITY STANDARDS

In this part, information security standards are addressed. The standards of Control Objectives for Information and Related Technology, The Information Technology Infrastructure Library and ISO/IEC 27001:2013 are selected and explained in detail.

3.1. COBIT

Control Objectives for Information and Related Technology, which is shortly known as COBIT, enables an organization to adopt an Information Technology (IT) governance. COBIT is one of the most applied information security standards worldwide in the area of information technology. In COBIT, there are a set of control objectives and practices which define what to do in order to establish and maintain a successful IT performance.

COBIT is an IT governance framework, and it helps managers to bridge the gap between control requirements, business risks and technical and security issues. It is a comprehensive set of resources that contains all the needs of information organizations to adopt and IT governance and control framework (COBIT Control Practices, 2007, pg. 7). The IT Governance areas of concentration are listed below (Susanto et. al., pg. 25):

- Strategic Alignment: Ensures the relationship between business and IT plans.
- Value Delivery: Ensures the benefits gathered through IT.
- Resource Management: Focuses on making optimal investments and managing the IT resources such as applications, information, infrastructure and people.
- Risk Management: Focuses on the risks that organizations face and searches for ways to eliminate them.

- Performance Measurement: Deals with implementation of strategies, completion of projects, usage of resources, delivery of service and process performance.

3.1.1. The History of COBIT

COBIT was first published in 1996 by Information Systems Audit and Control Association which is shortly known as ISACA. ISACA is an international association which is composed of professionals who work on information technology. The association was established in 1967. It was first located in Los Angeles. Nowadays, it has a lot of members in more than 100 countries. The members of the organization have a special certificate which is accepted internationally. The members of the association provide education, knowledge and information and also share their resources in many countries for other users. These volunteer professionals work on COBIT continuously in order to improve it. As a result, in 1998 and 2000, second and third versions were published, respectively. In 2005, a fourth version was published. Nowadays, COBIT is accepted and used worldwide for information technology governance and controls.

3.1.2. Overview of COBIT

3.1.2.1. Mission

The mission of COBIT is defined basically as researching, improving, sharing and promoting internationally accepted IT governance control framework for adoption by users (COBIT 4.1 Excerpt, pg. 9).

3.1.2.2. The Contribution of COBIT

COBIT interconnects business requirements and IT goals. COBIT organizes IT activities into a process model and identifies the IT resources to be focused. It also identifies the control objectives and practices which should be taken into consideration to guide the managers (IT Assurance Guide – Using COBIT, pg. 9).

3.1.2.3. The Benefits of Applying COBIT

COBIT provides several benefits to different parties. Management can determine its IT system controls and apply these controls and practices easily. They can also organize its resources effectively and make better IT investments based on the projects which will provide more benefits to the organization in the long term.

COBIT increases the efficiency of IT processes visibly. By being aware of the auditing controls and practices, IT personnel know what they are expected to do. Thus they can improve the operations they perform. COBIT is a very important guide for IT personnel. By applying COBIT, IT personnel can add value to the organization.

COBIT is developed by many IT professionals and auditors as mentioned before. Nowadays, it is accepted internationally and applied in many countries by authorities. COBIT is also vital for auditors. Because of the fact that all processes and controls are detailed in the standard, auditors know which controls should be focused on and which actions should be taken.

3.1.2.4. COBIT – IT Assurance Guide

IT Assurance Guide is prepared in order to explain how to use COBIT's processes and control objectives in organizations. As mentioned in the guide, assurance professionals are focused on primarily, but it can also be useful for IT professionals.

3.1.3. The Framework of COBIT

3.1.3.1. The Characteristics of the COBIT Framework

The characteristics of the COBIT framework are categorized as follows (Sheikhpour and Modiri, 2012a, pgs 15-16);

- Business-Focused: COBIT focuses on business orientation. It makes contributions to IT service providers, users, auditors, and also management and process owners. As seen, it has a wide range of service to different parties. Management and control of information are vital in COBIT. Quality, security and fiduciary requirements while delivering information should be considered.

- Process-Oriented: In version 4.1 of COBIT, there are 34 processes and in each of the processes a number of control objectives take place. There are 210 control objectives in four domains. These domains are categorized as:

1- Plan and Organize (PO)
2- Acquire and Implement (AI)
3- Deliver and Support (DS)
4- Monitor and Evaluate (ME)

- Control-Based: In each of 34 processes, various control objectives are defined. Status of the organization is evaluated based on the control objectives and according to the obtained results; needed actions are taken in order to eliminate the problems that can be faced and increase the effectiveness of the operations.

- Measurement-Driven: Every organization should be aware of its IT systems and required controls and management level. Management should question the organization's status quo and measure what they are and where they want to be. After making this evaluation, it is essential to monitor the improvements made.

3.1.3.2. COBIT Framework Model

In each domain of COBIT, there are different control objectives which help an organization to have a successful information technology system.

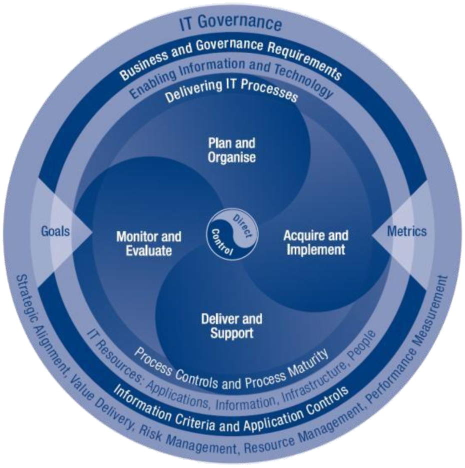

IT Governance
Business and Governance Requirements
Enabling Information and Technology
Delivering IT Processes
Plan and Organise
Goals
Monitor and Evaluate
Direct Control
Acquire and Implement
Metrics
Deliver and Support
Process Controls and Process Maturity
IT Resources: Applications, Information, Infrastructure, People
Information Criteria and Application Controls
Strategic Alignment, Value Delivery, Risk Management, Resource Management, Performance Measurement

Figure 3.1 : Overall COBIT Framework
Source : Powertech, 2010.

As seen in Figure 3.1, there are four areas which are related to goals and metrics. Each area contains compatible sets of different processes. For each of the process, scopes and purposes are detailed in COBIT in order to guide users. Each process is defined shortly as explained in IT Assurance Guide as set forth below.

3.1.3.2.1. Plan and Organize (PO)

There are 10 processes in the Plan and Organize domain. They are listed as:

PO1 - Define a Strategic IT Plan

PO2 - Define the Information Architecture

PO3 - Determine Technological Direction

PO4 - Define the IT Processes, Organization and Relationships

PO5 - Manage the IT Investment

PO6 - Communicate Management Aims and Direction

PO7 - Manage IT Human Resources

PO8 - Manage Quality

PO9 - Assess and Manage IT Risks

PO10 - Manage Projects

According to the Plan and Organize domain of COBIT 4.1, a strategic plan is defined which is compatible with business strategies and priorities. Information architecture is established in order to maintain reliable and secure information. The technological direction is determined to support the business. An IT organization is defined, and relationships and processes are established. IT-enabled investment programs are generated. The aims and direction of management are recognized by everyone in the organization. As people are important assets, IT human resources are managed properly. A quality management is developed to develop processes and standards. A risk management framework is established to understand the level of IT risks, mitigation strategies and residual risks. A program and project management framework is created to coordinate all the projects.

3.1.3.2.2. Acquire and Implement (AI)

There are 7 processes in the Acquire and Implement domain. They are listed as:

AI1 - Identify Automated Solutions

AI2 - Acquire and Maintain Application Software

AI3 - Acquire and Maintain Technology Infrastructure

AI4 - Enable Operation and Use

AI5 - Procure IT Resources

AI6 - Manage Changes

AI7 - Install and Accredit Solutions and Changes

According to the Acquire and Implement domain, automated solutions are identified in order to minimize the costs to acquire and implement solutions to achieve the organization's goals and objectives. Application software is acquired and maintained to support business operations with proper automated applications. The technology infrastructure is acquired and maintained to support business applications. The production of documentation and user manuals is required, and training of employees is provided to enable proper use of applications and infrastructure. IT resources such as employees, hardware, software and services are procured. All changes are managed properly by logging, assessing and authorizing before implementation. In order to understand whether operational systems are in line with the expected outcomes, proper testing is done.

3.1.3.2.3. Deliver and Support (DS)

There are 13 processes in the Deliver and Support domain. They are listed as:

DS1 - Define and Manage Service Levels

DS2 - Manage Third-party Services

DS3 - Manage Performance and Capacity

DS4 - Ensure Continuous Service

DS5 - Ensure Systems Security

DS6 - Identify and Allocate Costs

DS7 - Educate and Train Users

DS8 - Manage Service Desk and Incidents

DS9 - Manage the Configuration

DS10 - Manage Problems

DS11 - Manage Data

DS12 - Manage the Physical Environment

DS13 - Manage Operations

According to the Deliver and Support domain of COBIT, levels of services are defined and managed to support alignment between IT services and related business requirements. A third party management process is established by defining the roles and responsibilities of each party. The capacity and performance are managed by evaluating the performance and capacity of IT resources on a regular basis. IT continuity plans, offsite backup storage and regular continuous plan training are developed to provide continuous IT services.

A security management process is established to maintain information integrity and IT assets protection. By having an effective management system, security incidents are minimized. All the costs are identified, and a fair system of allocation is created. All users are educated and trained on a regular basis. With effective training, user errors are minimized and productivity is increased. An incident management system is developed to respond to IT user problems on time. Establishing a service desk is vital for incident resolution. A configuration management system is developed to minimize production issues and resolve them.

An effective management system involves identifying and classifying the problems. A data management system is created to provide business data quality, timeliness and availability. The physical environment is managed by using the proper facilities, selecting the processes for controlling environmental factors, monitoring physical access and understanding the physical site requirements. All the operations of an organization are managed to enable the integrity of data, reduce the delays of business and operating cost of IT.

3.1.3.2.4. Monitor and Evaluate (ME)

There are 4 processes in the Monitor and Evaluate domain. They are listed as:

ME1 - Monitor and Evaluate IT Performance

ME2 - Monitor and Evaluate Internal Control

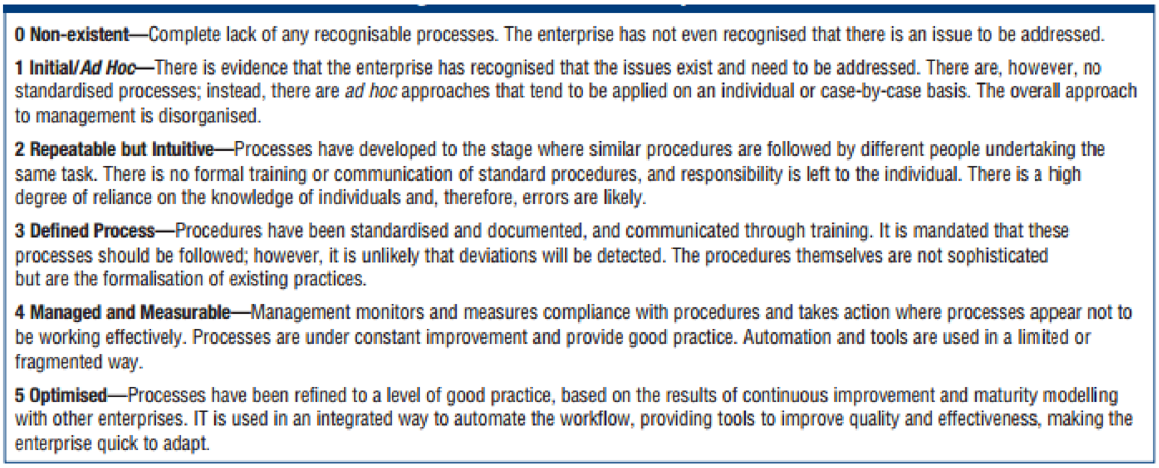
ME3 - Ensure Compliance with External Requirements

ME4 - Provide IT Governance

According to the Monitor and Evaluate domain of COBIT, IT performance is monitored and evaluated to understand whether everything done in the organization is in line with the established policies, standards and procedures. After developing an effective monitoring process, it is time to establish an internal control programme. Internal control helps an organization to be in line with the current laws and regulations. A review process enables to be compatible with external requirements such as laws, regulations and other requirements. An effective governance framework is established by the existence of defined processes, roles, responsibilities and organizational structure.

3.1.4. COBIT Maturity Model

According to COBIT, each organization should have a maturity level based on the evaluations made. It shows the status of the internal control environment. By using this model, an organization can position itself based on internal control. In the Maturity Model, several questions are developed for each maturity level by auditors. During the auditing period, evidence is collected by interviewing the IT employees and evaluating the documents in the process. An auditor can make a maturity calculation by the obtained results from the maturity levels of the IT processes. The alignment level is assessed by using the maturity levels (Tanuwijaya and Sarno, 2010, pg. 80).



0 Non-existent—Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.

1 Initial/*Ad Hoc*—There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are *ad hoc* approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.

2 Repeatable but Intuitive—Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.

3 Defined Process—Procedures have been standardised and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.

4 Managed and Measurable—Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

5 Optimised—Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

Figure 3.2 : Generic Maturity Model
Source : COBIT 4.1 Framework - Control Objectives - Management Guidelines - Maturity Models (Pg. 19)

The generic maturity model is shown in Figure 3.2. As seen, there is a 0-5 scale which ranges from non-existent to optimized. In the non-existent level, processes are not established and applied. In the initial/ad hoc level, processes are not organized and standardized. In the next level, which is repeatable but intuitive, there is a regular pattern. In the defined process level, processes are documented properly and communicated to everyone in the organization. In the managed and measurable level, processes are managed and measured in order to provide compliance and take actions to make them work effectively. The aim of organizations is to reach to the optimized level. When processes are established and applied properly and best practices are followed, it is possible to have an optimized capability.

3.2. ITIL

The Information Technology Infrastructure Library (ITIL) is a group of the best practices, applications and experiences for information technology services governance. Organizations aim to provide business value to their stakeholders by using the most effective information technology services. ITIL helps an organization to be aware of the value created through these services (Sheikhpour and Modiri, 2012b, pg. 2170).

ITIL which is known as an information library, encourages quality computing services in the area of information technology. Nowadays, ITIL is accepted internationally and applied in thousands of organizations which have different sizes and operates in various sectors worldwide.

3.2.1. The History of ITIL

In the late 1980s, the British Government elected the Central Computer and Telecommunications Agency (CCTA) to establish a structure in order to manage the British government’s and the private sector’s information technology sources effectively and securely. In 2000, CCTA renamed itself as Office of Government Commerce which is shortly known as OGC. By this way, the first version of ITIL was established by OGC in order to manage the British government’s and the private sector’s information technology resources. In 2000, version two of ITIL was released by the Office of Government Commerce. With the usage of ITIL by Microsoft, its popularity was increased sharply. In 2007, version three of ITIL was published. ITIL 2007 is updated in 2011. A lifecycle approach to service management was mentioned in the new version (Mathew and Basel, 2012, pg. 27). Since 2013, it has been owned by Axelos Ltd.

3.2.2. Overview of ITIL

3.2.2.1. The Users of ITIL

ITIL is used worldwide such as (ITIL®: the basics, 2013, pg. 4);

- Large technology companies: Microsoft, Hewlett Packard, Fujitsu, International Business Machines
- Retailers: Target, Walmart and Staples
- Financial services companies: City Bank of America
- Entertainment entities: Disney
- Manufacturers: Toyota, Bombardier
- Life sciences companies: Eli Lilly, Pfizer

3.2.2.2. Implementation of ITIL

There are a set of processes in ITIL. The roles and responsibilities of all parties are clear, which means that everyone in the organization is aware of what they are expected to do. Procedures for operating, planning and reporting are established. Companies mostly implement ITIL together with other practices. In order words, it becomes more sufficient when other standards are used in line with ITIL. The practices which can be used together with ITIL are (Marquis, 2006, pg. 51);

- Project Management and a Continuous Service Improvement Program (CSIP)
- Appropriate Goal Setting Through a Process Maturity Framework (PMF)
- Rigorous Auditing and Reporting Through a Quality Management System (QMS)

3.2.2.3. The Core Books of ITIL

In the first version of ITIL, the processes were defined in thirty books. In the updated version of ITIL, which was ITIL v2, there were seven books. Currently, there are five core books of ITIL. These books contain the stages of the service lifecycle. The sixth book, which is Official Introduction gives detailed information about the core books and makes an entrance to Information Technology Service Management (ITSM). The guide also describes the key principles of ITSM.

3.2.2.4. The ITIL Service Lifecycle

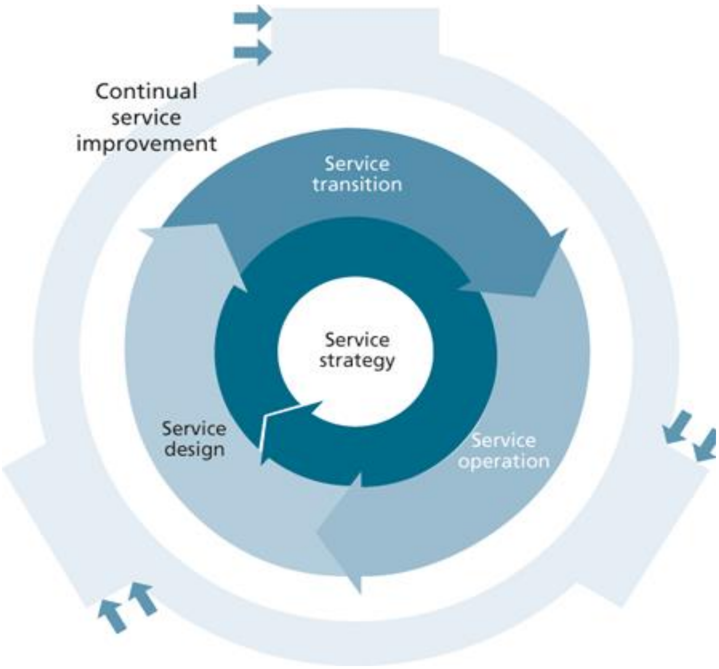


Figure 3.3 : The ITIL Service Lifecycle
Source : http://www.best-management-practice.com/serviceOperation2011_demo/

The ITIL Service Lifecycle is shown in Figure 3.3. ITIL is organized based on the service lifecycle which contains service strategy, service design, service operation, service transition and continual service improvement. As seen in the lifecycle there are five phases starting with service strategy and interrelated to other phases.

3.2.3. The Components of ITIL

ITIL is composed of five key principles:

- Service Strategy
- Service Design
- Service Operation
- Service Transition

- Continual Service Improvement

In each component of ITIL, there are a set of processes which are related and linked to each other. ITIL describes the activities which take part in the processes but do not suggest how to implement them.

3.2.3.1. Service Strategy

The purpose of service strategy is to define the perspective, position, plans and patterns that a service provider needs to achieve objectives. The processes in service strategy are listed as (ITIL Service Strategy, 2011):

- Strategy Management for IT Services
- Financial Management for IT Services
- Business Relationships Management
- Service Portfolio Management
- Demand Management

Strategy Management for IT Services manages all strategy plans. It ensures that strategy plans are translated into tactical and operational plans. Financial Management for IT Services is related to management of functions and processes which are responsible for IT service provider's budgeting, accounting and charging necessities. Business Relationship Management links service providers and customers at strategic and tactical levels. Service Portfolio Management (SPM) contains the proactive management of the investments done in the service lifecycle. It also contains the concept, design and transition services and live services which are described in different service catalogues and retired services. The purpose of Demand Management is influencing of customer demands on services and defining the capacity to supply the demands (An Introductory Overview of ITIL 2011, pgs. 17-19).

There are three objectives of service strategy which are listed as (Malone, Menken and Gerard, 2009, pg. 25):

- Service strategy helps an organization in designing, developing and implementing service management as a strategic asset. It also enables the growth of the organization.
- Service strategy helps an IT organization in developing the capability to handle the costs and risks related to activities which are related to the service portfolio.
- Service strategy helps an organization to describe the IT strategic objectives.

There are four P's of strategy. The first one is perspective, which defines the distinctive vision and direction. The second P is position, which is the basis on which the provider will compete. The third P is plan, which defines how the providers will active the vision. The last P is pattern, which is the fundamental way of doing things (An Introductory Overview of ITIL 2011, pgs. 13-14).

3.2.3.2. Service Design

Another stage in the service management lifecycle is service design. Service design component of ITIL provides guidance for the design of services and service management practices. The processes in service strategy are listed as (ITIL Service Design, 2011):

- Design Coordination
- Service Catalogue Management
- Service Level Management
- IT Service Continuity Management
- Supplier Management
- Availability Management
- Capacity Management
- Information Security Management

Design Coordination ensures that the goals and objectives of the service design are achieved. Service Catalogue Management provides information on all of the agreed services and makes them available for the people who are permitted to access them. Service Level Management aims to ensure that IT service is provided for all information technology services and future services are delivered to defined targets. The purpose of Capacity Management is defined as concentration and management of business, services and components. Availability management provides focus and management for resource, component and service availability. IT Service Continuity Management maintains the proper recovery capability with IT services to meet needs and requirements. The process of Information Security Management aims to manage information in all activities of the organization. The security objectives are accomplished when availability, confidentiality and integrity of information are accomplished. The purpose of Supplier Management is to ensure that all suppliers and services meet organization's needs, objectives and expectations (ITIL Service Design, 2011).

The four P's of service design are; people, products, processes and partners. People are human resources to support the service. Products are services, tools and technology which support the services. Processes are the activities which supply the information technology services. Partners provide services required to support the service. All of them should be involved in information technology services for effective and efficient use of service design.

3.2.3.3. Service Transition

Service transition concentrates on applying all aspects of the service. The objectives of service transitions are (ITIL Service Transition, 2011):

- Planning and managing service changes
- Managing risks
- Deploying service releases into supported environments
- Setting correct expectations on the performance and use of services
- Ensuring the creation of expected business value by service changes
- Providing good-quality knowledge and information about services and service assets

The processes that take place in the service transition publication are listed:

- Service Asset and Configuration Management
- Change Management

- Knowledge Management
- Transition Planning and Support
- Release and Deployment Management
- Service Validation and Testing
- Change Evaluation

Service Asset and Configuration Management (SACM) deals with all assets that take place in the lifecycle. The policy of service asset and configuration establishes the framework and key principles against which assets and configurations are developed and maintained (UCISA ITIL: A Guide to Service Asset and Configuration Management). The Change Management process ensures that any changes in all stages of the service management are recorded, evaluated and documented. With an effective management system, changes are handled properly. Knowledge Management provides the fit between person and knowledge. Right person and right knowledge should league together at the right time to deliver and support the services. The Transition Planning and Support process plans and organizes resources to meet the requirements in service strategy. It also handles the risks of failure and distortions through the activities. The Release and Deployment Management process deals with whole assembly and implementation of services for operational use. The Service Validation and Testing process aims to provide unbiased evidence that the new or changed services promote the requirements of the business (An Introductory Overview of 2011, pgs. 33-37).

3.2.3.4. Service Operation

Service Operation provides guidance to maintain stability in service operation, allowing for changes in design, scale, scope and service levels. The processes in the service operation publication are listed below (ITIL Service Operation, 2011):

- Event Management
- Incident Management
- Request Fulfillment
- Problem Management
- Access Management

Event management purposes to manage events throughout the lifecycle by determining the corrective actions. Incident management puts emphasis on reintegrating accidentally degraded/disrupted services to users as quickly as possible to avoid any adverse impact that may occur. On the other hand, Problem Management contains root-cause analysis which is used to define and resolve the incident causes. It involves the proactive activities to define and prevent the problems or incident that may occur in the future. Request fulfillment provides information about the availability of service and deals with service requests of users. With a successful Access Management process, it is possible to allow authorized users to access IT services, data and other assets (An Introductory Overview of ITIL 2011, pgs. 40-44).

3.2.3.5. Continual Service Management

Continual Service Management creates and maintains value for customers by having better strategy, design, transition and operation of services. The practices, principles and methods of quality management, change management and capability improvement are associated in continual service management volume. There are 7 steps in this component of ITIL that are listed below (ITIL Service Improvement, 2011):

1. Identifying the strategy for improvement
2. Define what you will measure
3. Gather the data
4. Process the data
5. Analyze the information and data
6. Present and use the information
7. Implement improvement

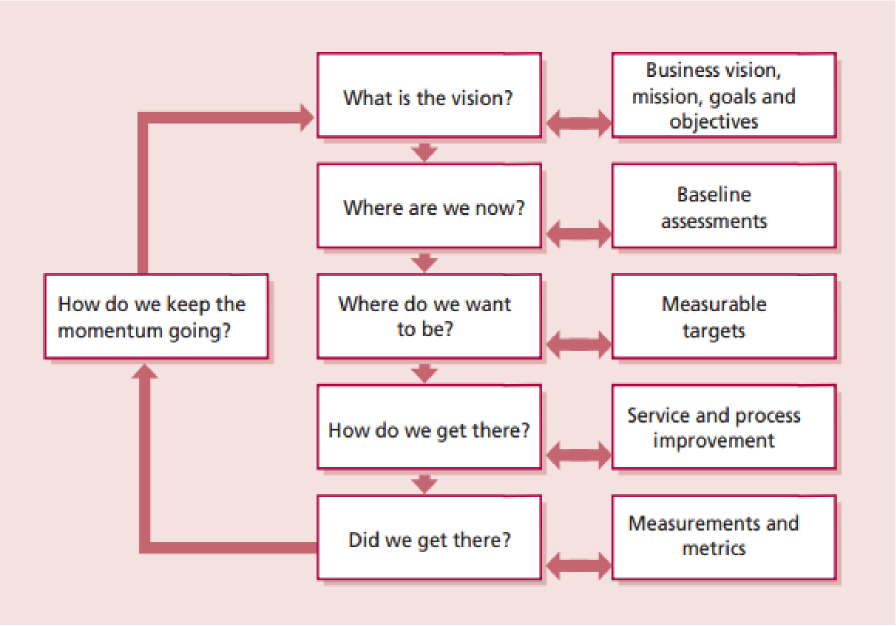


Figure 3.4 : The Continual Service Improvement Approach
Source : An Introductory Overview of ITIL, 2011

The Continual Service Improvement Approach is shown in Figure 3.4. The vision contains business vision, mission, goals and objectives. By making assessments, an organization can understand where it is. Measurable targets define the point where the organization wants to be in the future. Service and process improvements show the ways to reach the measurable targets. With proper evaluations, it is possible to understand whether the targets are achieved or not.

3.3. ISO/IEC 27001:2013

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) built a system in order to establish a standardization. These two institutions are consolidated and worked under the name of ISO/IEC. The objective is to prepare International Standards which are accepted internationally.

The focal point of ISO 27001 is defined as the requirement for planning, implementation, operation and continuous monitoring and development of a process-oriented information security management system (Disterer, 2013, pgs. 92-100).

3.3.1. The History of ISO 27001

The title of the standard is "Information technology— Security techniques — Information security management systems — Requirements". The first edition of the Standard which is ISO 27001 was published by the Joint Technical Committee ISO/IEC JTC 1 in 2005. The second edition, which is ISO 27001:2013, canceled and replaced the first version of the standard. Contrary to ISO 27001:2005, the ISO 27001:2013 does not contain the Plan-Do-Check-Act cycle. The new version focuses on measuring and evaluating the organization’s information security management system performance and activities.

3.3.2. The Scope of ISO 27001

ISO 27001:2013 defines the requirements to establish, implement, maintain and improve an effective information security management system. The standard contains requirements for the evaluation and treatment of information security risks tailored to the needs of the organization. The requirements that are established in the standard are generic and are workable for all organizations.

3.3.3. The Framework of ISO 27001

3.3.3.1. Context of the Organization

According to the Standard, an organization should determine its purpose and define both external and internal issues that are related to determined purposes. Organizations should also form an effective Information Security Management System (ISMS) in line with the Standard. After forming the system, relevant parties and their requirements such as legal and regulatory requirements and contractual obligations are determined.

3.3.3.2. Leadership

Top management of the organization should demonstrate leadership and commitment concerning the ISMS. An information security policy shall be formed which is in line with the organization’s direction, contains the objectives of information security and commitment to provide applicable requirements. The policy is expected to be documented, communicated and available. Top management of the organizations is the competent authority to assign the duty and responsibility based on information security.

3.3.3.3. Planning

ISO 27001 instructs organizations to determine the risks and opportunities they have. An organization should determine and implement an information security risk assessment process which contains information security risk criteria and ensures that it provides coherent, acceptable and comparable outcomes. The owner and level of risks are determined. Information security risks are analyzed and prioritized for risk treatment. Information security objectives should be in line with information security policy, measurable, communicated and updated regularly.

3.3.3.4. Support

According to the Standard, the resources which are needed for the information security management system are defined and provided. The employees of the organization are expected to be aware of the information security policy and understand it properly. ISMS is communicated both internally and externally.

3.3.3.5. Operation

As defined in the standard, an organization should plan, implement and control the processes which help to meet the requirements in order to provide an effective information security. An organization should also establish an information security risk treatment plan and apply it properly.

3.3.3.6. Performance Evaluation

The information security performance and the effectiveness of ISMS should be monitored and evaluated by the organization. It is expected to have internal audits that give information about the information management system of the organization. The controls done by internal auditors should be regular. The information security management system should be reviewed by top management on a regular basis to reduce or eliminate any trouble that the organization can be faced with. While making evaluations, previous management reviews and feedbacks on the performance of information security are taken into consideration.

3.3.3.7. Improvement

As mentioned in the Standard, the suitability, adequacy and effectiveness of an information security system is expected to improve continuously. If there is nonconformity, corrective actions should be taken. After that, the effects and effectiveness of corrective actions are evaluated.

3.3.4. Control Objectives and Controls

There are several control objectives and controls in ISO 27001 that organizations implement to have an effective information security management system. There are 14 control objectives and in each objective there are several controls. All of the control objectives and controls are detailed in the standard.

The control objectives are listed below:

- A.5 Information Security Policies
- A.6 Organization of Information Security
- A.7 Human Resource Security
- A.8 Asset Management
- A.9 Access Control
- A.10 Cryptography
- A.11 Physical and Environmental Security
- A.12 Operations Security
- A.13 Communications Security
- A.14 System Acquisition, Development and Maintenance
- A.15 Supplier Relationships
- A.16 Information Security Risk Management
- A.17 Information Security Aspects of Business Continuity Management
- A.18 Compliance

ISO 27001:2013 Standard consists of 14 domains of control objectives and controls. According to the Standard, an organization is expected to do/be in each domain as:

- Information Security Policies: A group of policies are established and implemented for information security. These policies are reviewed on a regular basis for suitability, adequacy and effectiveness.

- Organization of Information Security: Top management of the organization defines and assigns the roles and responsibilities for information security. Risks are managed for the security of teleworking and mobile devices. In order to maintain it, a policy is established and needed supporting security measures are taken.

- Human Resource Security: Employees and other parties of the organization are aware of their roles and responsibilities. They are required to understand what they are expected to do. A fit between employees/other parties and assigned roles and responsibilities are essential. All employees in the organization are responsible for information security. On the other hand, management has to provide education and training for the employees to increase awareness based on information security.

- Asset Management: The assets of an organization are defined and assigned to users. The assets are returned when employees or other parties terminate their employment, contract or agreement. Information is classified based on its criticality and sensitivity. A classification scheme is established in the organization. After establishing the scheme, procedures for information labelling are developed and applied. Management of removable media is ensured by proper procedures. While transferring the media physically, information is protected against any unauthorized access, abuse or breakdown.

- Access Control: Access control policy that is in line with information security is established, documented and reviewed on a regular basis. User access is managed properly to prevent any unauthorized access. System and application access control are provided for systems' and applications' security.

- Cryptography: A policy is established for the proper use of cryptographic controls. In this way, it is possible to enable the protection of information. Key management contributes to use and protects cryptographic keys properly along the lifecycle.

- Physical and Environmental Security: Within an effective physical and environmental security process, physical security perimeters and entry controls are defined. External and environmental threats are determined and needed security actions are taken. Employees should be provided to work in secure areas. Assets of the organization are protected against loss, damage or robbery.

- Operations Security: Operating procedures are documented and ready for use by the people who need them. All of the changes which may influence information security are controlled. Controls against malware are established and implemented to protect information and service area. In order to prevent loss of data, backup copies are taken that are compatible with the established backup policy. Events are logged and reviewed regularly. Audit controls for information systems are established.

- Communications Security: Information in systems and applications are protected by effective management of networks. Information can be transferred either within the organization or to outside of the organization. To ensure this, information transfer policies and procedures are established.

- System Acquisition, Development and Maintenance: Information security is vital in information systems. Because of this fact, it is important that information involved in the systems is protected properly. All security requirements are considered while protecting the systems. A security developments policy is established. Control policies are defined and applied for the changes done in the systems. After taking these actions, the functionality of security is tested and gathered data is protected and controlled properly.

- Supplier Relationships: Information security policy is also defined and implemented for supplier relationships. The policy contains the risks that are related to the access of suppliers to the assets that the organization holds. Changes to supplier services are managed effectively.

- Information Security Incident Management: Management of the organization defines the responsibilities and procedures in order to respond to the security incidents immediately. The information security events and weaknesses are reported. It is vital to learn from information security incidents to avoid any event that may occur in the future.

- Information Security Aspects of Business Continuity Management: Information continuity plans are defined, established and documented. In the case of any crisis or disaster, the organizations implement information security continuity plans. It is critical to affirm, revise and evaluate the controls which are established for information security continuity on a regular basis to be sure that they are effective in the case of any adverse situation.

- Compliance: Requirements for practicable legislation and regulations related to information security are identified. The organization applies them and thus becomes compatible with the requirements of security. Information security reviews are important from the point of being independent. The reviews done by authorized people are in compliance with established policies, procedures and standards. The systems and process are reviewed on a regular basis.

3.3.5. The Other ISO Standards

The information security standards of ISO are gathered under the roof of ISO 27000 series. The series is also known as the ISMS Family of Standards. 27001 takes place in the ISO 27000 series. There are nearly 40 related standards in the series that are related to ISO 27001 and ISMS. Some of the standards are listed as (http://www.iso27001security.com/) ;

ISO 27000: An overview of information security management systems, and defines related terms.

ISO 27002: Guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization.

ISO 27003: Help and guidance in implementing an ISMS.

ISO 27004: Provides guidance on the development and use of measures and measurement for the assessment of the effectiveness of an implemented information security management system and controls, as specified in ISO 27001.

ISO 27005: Guidelines for information security risk management in an organization, specifically supporting the requirements of an information security management system defined by ISO 27001.

ISO 27006: Guidelines for the accreditation of organizations which offer certification and registration with respect to an ISMS.

ISO 27007: Guidance for auditing an Information Security Management System against ISO 27001.

ISO 27008: Guidelines for Information Security management auditing.

In the next part, decision making and Analytic Hierarchy Process method will be examined in detail.

CHAPTER IV

DECISION MAKING AND ANALYTIC HIERARCHY PROCESS

In this part, decision making process is considered in detail. Analytic Hierarchy Process is applied in complex situations. The method, its advantages and disadvantages, steps and applied software package are addressed.

4.1. DECISION MAKING PROCESS

4.1.1. The Concept of Decision and Decision Making

A decision is described as a choice made within the framework of various cognitive actions with the intention to produce satisfying results (Yates, Veinott and Patalano, 2003, pg. 13). Decision making is defined as s process of selecting the most appropriate alternative based on at least one purpose or criteria within a set of options (Dağdeviren and Eren, 2001, pg. 42). People make decisions among several possible alternatives in each part of their lives. At the end of each decision making process, there is a final choice which is selected by decision maker. Making good decisions is one of the most important functions of management and it is vital for organizations to focus on the process properly. Managers select the best option among various alternatives to fulfill the purpose that was established before. In order to make good decisions, different kinds of knowledge, information and data are needed. They concern the following items (Saaty, 1994, pg. 21);

- Details about the problem,
- The people or actors who take part in the process,
- Established policies and objectives,
- The influences which affect the outcomes,
- The time frame, scenarios and limitations.

There are various factors that may influence the decision maker. For instance, a person's culture, subculture and social class as well as his or her self- image, reference groups and situational factors are important influencers/aspects in the decision making process of a buyer (Mescon, Bovee and Thill, 2002, pgs. 324-325).

According to Saaty (1997), a decision making process is composed of;

- Structuring a problem with a model that demonstrates the problem's key elements and the relationships between them,
- Showing judgments that reflect knowledge, feelings or emotions,
- Representing the judgments with meaningful numbers,
- Using the numbers to calculate the priorities of the elements in the hierarchy,
- Synthesizing the results to come up with an overall outcome,
- Analyzing sensitivity to changes in judgment.

4.1.2. Steps of the Decision Making

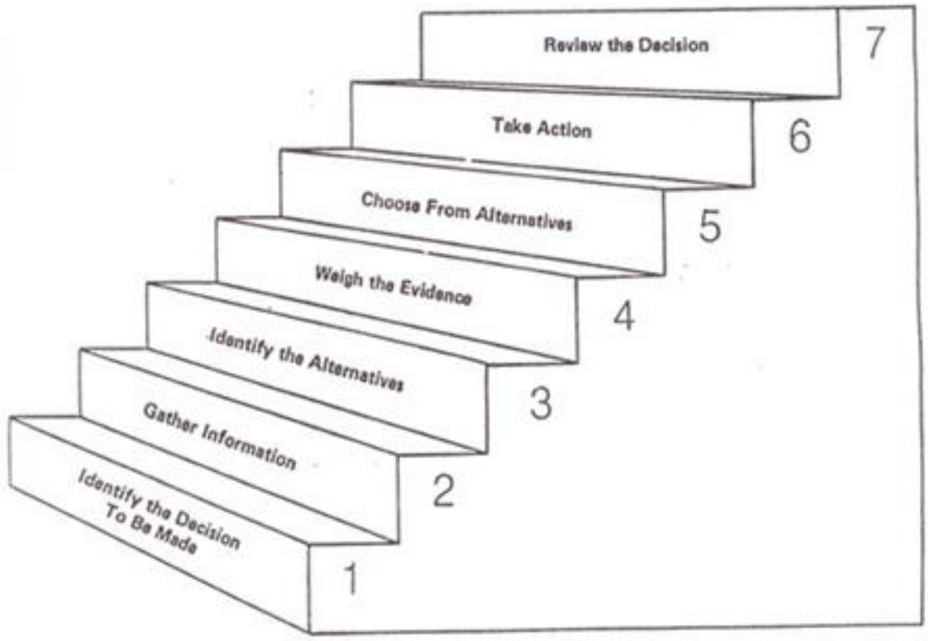


Figure 4.1 : Decision Making Steps
Source : http://www.umassd.edu/media/umassdartmouth/fycm/Decision_making_process.pdf

As seen in Figure 4.1, there are seven steps in the decision making process. These steps are described as (Lunenburg, 2010, pgs. 3-7);

4.1.2.1 Identification of the Decision

The first step in the decision making process is identifying the problem properly. Problem identification is the most important of the process. Establishing the goals and objectives are the basis of identifying the problem. A decision becomes effective when the established goals or objectives are achieved at the end.

Effective decision makers are aware of how important identifying the problem and understanding the situation of the problem is. Problem definition depends on the perception of decision maker. Well diagnosed problems are more important than the solution itself. Determination of the problem influences and increases the decision quality.

4.1.2.2. Gathering Information

After identifying the problem properly, it is time to gather information. Knowing what information is needed for the solution of the problem is important. Finding the ways of getting information is also essential. In order to gather information, internal and/or external work is required.

4.1.2.3. Identifying the Alternatives

This is one of the most important steps of the process. In this stage alternatives for solution are developed. After gathering information, several alternatives occur. All alternatives can be a potential for the solution. All possible alternatives are listed and being ready for the next step which is weighing the evidence in order to evaluate the alternatives. If there is only one alternative to achieve the established goals or objectives, it means that there is no need for decision making.

4.1.2.4. Evaluating the Alternatives

Each alternative is evaluated by deeply weighing the evidence. In this step satisfaction and feasibility of each alternative is analyzed. The basis of judgment is required to understand how close alternatives' consequences achieve the established goals or objectives of the decision makers.

Positive and negative aspects of each alternative are listed based on following items (Koçel, 2003, pg. 98);

- Technical feasibility,
- Cost of resources,
- Social and cultural suitability,
- Amount of needed resources for the implementation,
- Expected degree of results,
- Affection of other applications.

4.1.2.5. Choosing from the Alternatives

After evaluating the alternatives meticulously, the best alternative which supports and enables achieving the established goals or objectives is selected. It is also possible to select a combination of alternatives.

4.1.2.6. Implementing the Decision

Once all alternatives are evaluated and the best one is chosen by the decision maker, it is time to take action and implement the chosen alternative. The implementation of the decision is the result of the decision process accomplished by the decision maker.

4.1.2.7. Reviewing the Decision

Finally, the decision, its consequences and effectiveness are evaluated to identify whether the goals/objectives have been achieved. Evaluation is the vital component of the process because it enables an understanding of whether a new decision should be made or not. If the implemented decision does not achieve its goals or objectives, it means that there is a gap between expectations and the current situation. Several reasons ma cause this situation, including incorrectly defined problems, poorly evaluated alternatives or inappropriate implementation of the problem.

4.1.3. Types of Decision Making

Decisions are classified on different bases. The types of decision making are listed as;

4.1.3.1. Programmed and Non Programmed Decision Making

Programmed decisions are the decisions that are made repeatedly and on a routine basis. Therefore, they have developed rules or guidelines that are unconsciously applied in many daily-life situations. On the other hand, non-programmed decision making is required when non routine decisions are made, such as buying a new house. It is applied when there is not any a ready decision rule or guidelines. Intuition and judgment of the decision maker are very important in this kind of decision making. The decision maker makes decisions based on past experiences, immediate feeling or evaluation of the information at hand (George and Jones, 2003, pgs. 220-221). The information at hand can be based on single or multi-criteria.

4.1.3.2. Single-criteria and Multi-criteria Decision Making

Decision making is divided into two groups based on the criteria. In single-criteria decision making, there is only one criteria and purpose for the problem. It is easy to solve this kind of problems. Unfortunately, decision makers are aiming to optimize more than one purpose in real life, for that reason decision making process is becoming more complex. This situation causes the development of multi-criteria decision making methods (Subaşı, 2011, pg. 15).

Multi-Criteria Decision Making (MCDM) is used for structuring, planning and solving complex decisions. In this kind of decision making, there are several options present for the problem which needs to be solved. MCDM aims to select the most applicable alternative out of a group of alternatives. Alternatives with many criteria make it more difficult to solve the problem. MCDM enables making good decisions when choosing best alternative is highly complex. It has been applied in many areas. Making good decisions within this method can be achieved by analyzing the different scope for the criteria, weights for the criteria and selecting the best alternative using any multi criteria decision making techniques (Aruldos, Lakshmi and Venkatesan, 2013, pgs. 31-32).

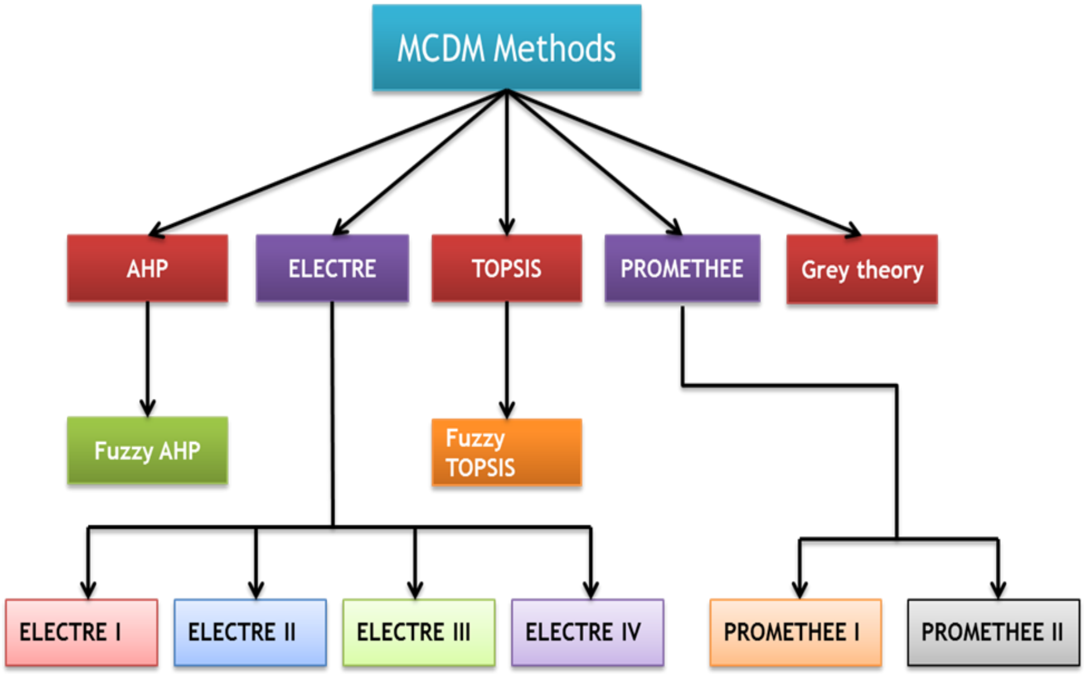


Figure 4.2 : Hierarchical Structure of MCDM Methods
Source: A Survey on Multi Criteria Decision Making Methods and Its Applications, 2013

Multi-criteria decision making methods have been shown in Figure 4.2. These methods are implemented to different applications and find the best solution to choose the best alternative. Figure 4.2 pictures the hierarchical structure MCDM methods and sorts of it. One of the methods is Analytic Hierarchy Process which compares different alternatives for different criteria. The next session describes the method based on literature review.

4.2. ANALYTIC HIERARCHY PROCESS

The Analytic Hierarchy Process (AHP) is first suggested by Myers and Alpert in 1968. It is developed as a model by Thomas L. Saaty in 1977 (Saaty, 1977). AHP method became one of the most applicable techniques used to solve multi-criteria decision problems (Dağdeviren, Akay and Kurt, 2004, pg. 132). In the method, the decision maker makes judgments on each criterion and defines a preference for each decision alternative using each criterion. After that, decision alternatives are ranked according to the decision maker’s expression on the overall performance (Anderson, Sweeney and Williams, 2005, pg. 732).

According to Saaty (2008), AHP is defined as a theory of evaluation through pair-wise comparisons and relies on the judgments of the decision maker to derive priority scales. AHP is one of the most applied methods in multi-criteria decision making. It is a scientific method which combines qualitative and quantitative criteria. The procedures of AHP can be applied both to individual and group decision settings (Lai, Wong and Cheung, 2002, pg. 135).

4.2.1. Advantages and Disadvantages of AHP

Analytic Hierarchy Process method is used in many situations. The method has several benefits. AHP is extending the scale from 1-9 to 1-9^n, where n stands for the number of clusters, reducing the number of comparisons and raising the problem of derivation method choice (Ishizaka, 2004).

The method is flexible, intuitive and easy to apply. It checks inconsistencies and by establishing a hierarchical structure it makes each criterion’s importance more evident. In this way, the decision maker can make pair-wise comparison and compare alternatives easily. On the other hand, in terms of disadvantages, the method can cause irregularities in ranking. Because of the nature of comparisons for rankings, the addition of alternatives at the end of the process may cause the final rankings to flip or reverse. AHP is mostly used in performance-type problems, resource management, corporate policy and strategy, public policy, political strategy, and planning (Velasquez and Hester, 2013, pg. 59).

4.2.2. The Axioms of AHP

According to Saaty, AHP is composed of four axioms which are listed as follows;

- Axiom 1: Pair-wise comparisons of two alternatives are done based on a criterion or sub-criterion on a ratio scale which is reciprocal.

- Axiom 2: The decision maker judges an alternative to be highly better than another based on a criterion.

- Axiom 3: The decision problem is structured in a hierarchy.

- Axiom 4: All criteria, sub-criteria and alternatives are located in the hierarchical structure.

4.2.3. Steps of AHP Method

There are five steps which should be followed while applying AHP method. These steps are shown in Figure 4.3.

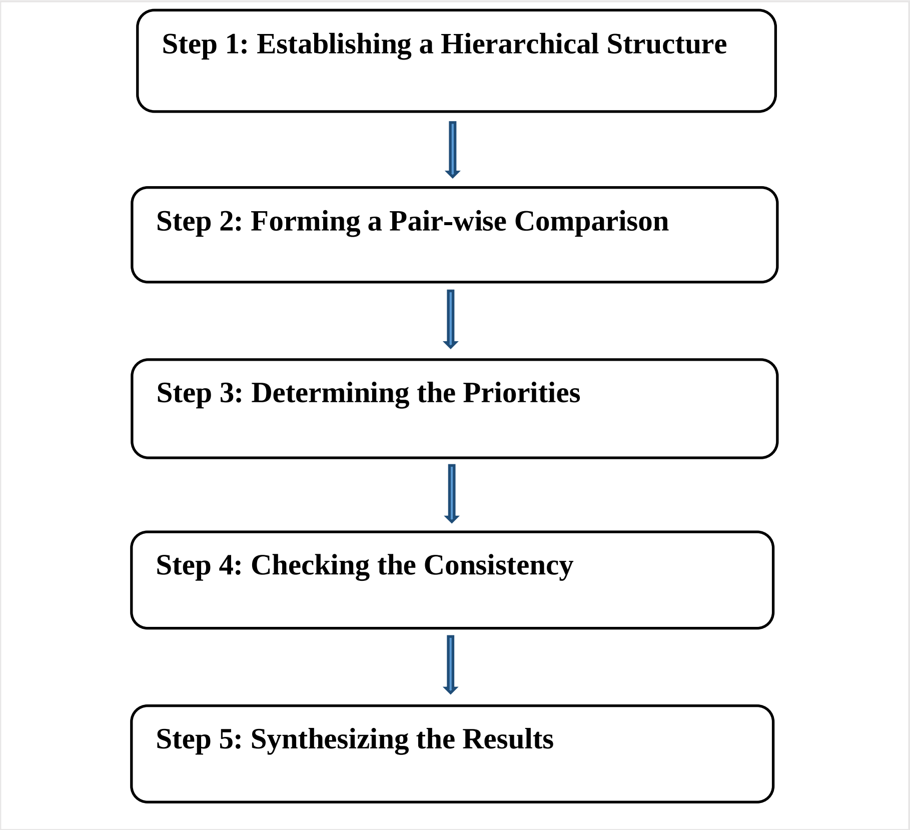

Step 1: Establishing a Hierarchical Structure
Step 2: Forming a Pair-wise Comparison
Step 3: Determining the Priorities
Step 4: Checking the Consistency
Step 5: Synthesizing the Results

Figure 4.3: Steps for AHP

The steps of the method are shown in Figure 4.3. The AHP consists of three main operations, including hierarchy construction, priority analysis and consistency verification (Ho, 2008, pg. 212). Their applications are described next.

4.2.3.1. Establishing a Hierarchical Structure

The first step of the AHP method is defining the problem and the objective. A hierarchical structure composed of objectives, criteria, sub-criteria and alternatives of the problem is established.

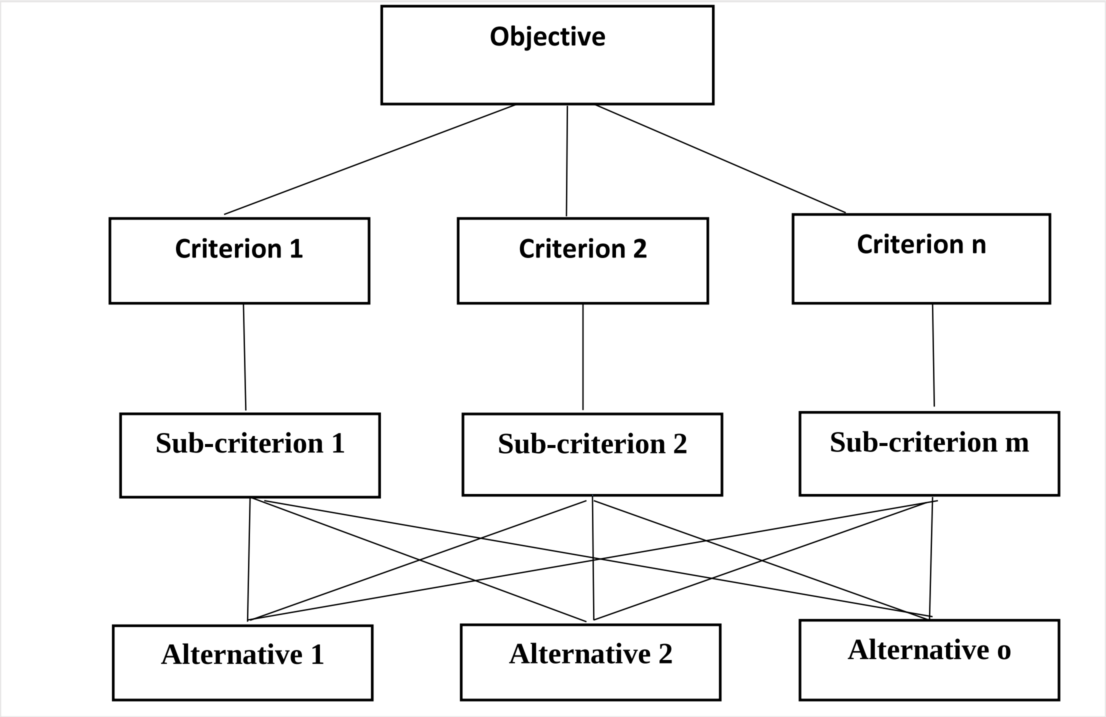


Figure 4.4: The Hierarchical Structure of AHP

Figure 4.4 shows the typical Hierarchical Structure of AHP. An objective is set based on the problem. In order to choose one of the alternatives, criteria and sub-criteria are evaluated. They should be in line with the objectives of the problem.

4.2.3.2. Forming a Pair-wise Comparison

In the second step two elements of the structure are compared at the same time. All criteria in the structure are compared one-by-one. In Table 4.1 and Table 4.2, pair-wise comparisons are shown.

Table 4.1: Pair-wise Comparison of Criteria

	Criterion 1	Criterion 2	…..	Criterion n
Criterion 1	C1/C1	C1/C2	…..	C1/Cn
Criterion 2	C2/C1	C2/C2	…..	C2/Cn
…..	….	…..	….	….
Criterion n	Cn/C1	Cn/C2	….	Cn/Cn

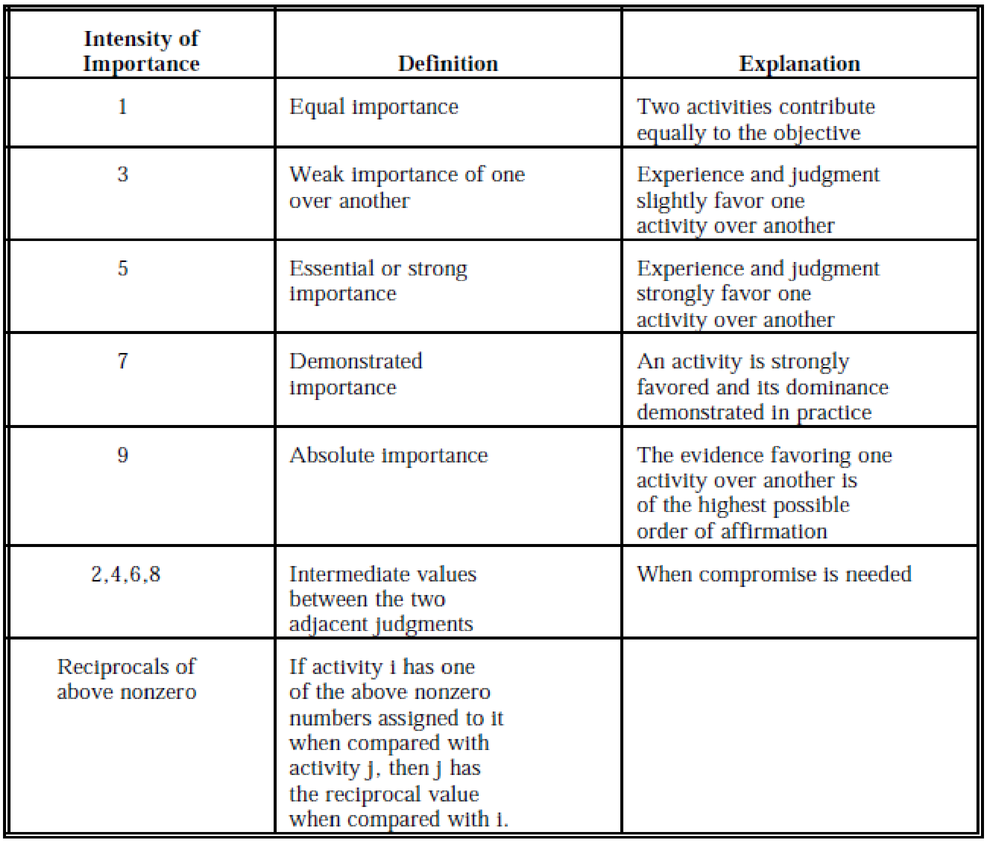
As seen in the Table, all criteria are compared one-by-one. The comparison of the same criteria is always 1. Saaty has established a scale for pair-wise comparison of criteria and alternatives. After comparing all criteria, alternatives are compared based on each criterion.

Table 4.2: Pair-wise Comparison of Alternatives Based on Criterion *m*

Criterion m	Alternative 1	Alternative 2	…..	Alternative n
Alternative 1	A1/A1	A1/A2	…..	A1/An
Alternative 2	A2/A1	A2/A2	…..	A2/An
….	….	….	….	….
Alternative n	An/A1	An/A2	….	An/An

There are (nxn) weight ratios where *n* stands for the compared elements. 1-9 scale of AHP is shown In Table 4.3.

Table 4.3: 1-9 Scale of Saaty (Saaty, 1980)



Intensity of Importance	Definition	Explanation
1	Equal importance	Two activities contribute equally to the objective
3	Weak importance of one over another	Experience and judgment slightly favor one activity over another
5	Essential or strong importance	Experience and judgment strongly favor one activity over another
7	Demonstrated importance	An activity is strongly favored and its dominance demonstrated in practice
9	Absolute importance	The evidence favoring one activity over another is of the highest possible order of affirmation
2,4,6,8	Intermediate values between the two adjacent judgments	When compromise is needed
Reciprocals of above nonzero	If activity i has one of the above nonzero numbers assigned to it when compared with activity j, then j has the reciprocal value when compared with i.	

According to the 1-9 scale of Saaty (1980), two criteria may have equal importance. In this case, the comparison has a scale of 1. If one element is extremely important than the other one, the comparison will have a scale of 9. According to the scale, values of 9, 8, 7, 6, 5, 4, 3, 2 and 1 are used. For the reverse comparison scale of 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8 and 1/9 are used. Based on Saaty's 1-9 scale, a criterion may have moderate importance, strong importance, very strong importance or extreme importance over another one. After accomplishing the pair-wise comparison of all criteria, the alternatives are compared according to each criterion.

4.2.3.3. Determining the Priorities

A measurement theory is used to establish the priorities of the hierarchy. This measurement evolves out of comparisons, particularly pair-wise comparisons (Wind and Saaty, 1980, pg. 645). Pair-wise comparisons have become interesting for many researchers. It is used to determine the relative importance of alternatives based on each criterion. In order to apply this method, the decision maker has to put his opinion about the alternatives, criteria and sub-criteria at a time (Triantaphyllou and Mann, 1995, pg. 37). According to Saaty, there are three steps in this stage to compute the eigen vector of a matrix as;

Step 1 : The values in each column are summed.

Step 2 : Each element of the matrix is divided by its column total.

Step 3 : The elements in each row are averaged to determine the priority of each criterion.

4.2.3.4. Checking the Consistency

AHP provides a measure of the consistency of the pair-wise judgments that are done by the decision maker. AHP allows for and also explicitly deals with inconsistencies. It provides a measure of the ratio of inconsistency (CR). CR demonstrates the degree to which each pair-wise comparison is consistent with the remainder of the comparisons. A mathematical approach is developed by Saaty which estimates weighing factors and priorities for the factors (Hummel, 2001, pg. 45).

A consistency ratio which is greater than 0.10 means that there is an inconsistency in the pair-wise comparisons. In this case, it is advised to re-evaluate the comparisons before proceeding. The steps needed to take for consistency are listed as follows (Anderson et al., pgs. 738-740);

Step 1 : Each value in the first column of the pair-wise comparison matrix is multiplied by the priority of the first item. This process is done for all columns and items one by one. Then, the values across the rows are summed up to get a vector of values labeled “weighted sum”.

Step 2 : The elements of the weighted sum vector which is calculated in Step 1 is divided by the corresponding priority of each criterion.

Step 3 : The average of the values obtained in the previous step are computed and showed by λmax.

Step 4 : The Consistency Index (CI) is calculated. CI is calculated by the following formula;

$$CI = \frac{\lambda \max - n}{n - 1}$$

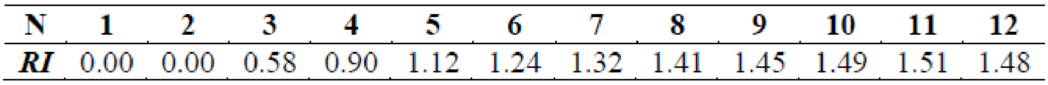
where *n* is the number of elements which are used in comparisons.

Step 5 : The Consistency Ratio (CR) is calculated. CR is calculated by the following formula;

$$CR = \frac{CI}{RI}$$

where RI is the consistency index of a randomly generated comparison matrix. RI depends on the compared number of elements. The values of RI are shown in Table 4.4.

Table 4.4: Random Consistency Index (Saaty, 1980)



N	1	2	3	4	5	6	7	8	9	10	11	12
RI	0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49	1.51	1.48

4.2.3.5. Synthesizing the Results

According to the model, if the consistency ratio is 0,10 or less, the pair-wise comparisons are evaluated as acceptable. In this situation, the next step of the method is synthesizing the results. The results obtained in the process are ranked from high to low. The alternative with the highest value is accepted as the optimal alternative for the decision.

4.2.4. The Expert Choice Package

The Expert Choice Package is developed by Thomas L. Saaty and Ernest Forman in 1983. The package is marketed by Decision Support Software. It helps to implement Analytics Hierarchy Process on a computer. After the decision maker enters criteria, sub-criteria, alternatives and pair-wise comparisons, Expert Choice automatically calculates the matrix and shows the overall priorities at the end. It also calculates the consistency index to evaluate the validity of the comparisons. In brief, Expert Choice is a software package which is used by decision makers to solve multi-criteria decision problems (Anderson et. al, pg. 743).

In next chapter, the implementation part of the study will take place. The information security standards based on selected criteria will be analyzed by using AHP method.

CHAPTER V

RESEARCH METHODOLOGY

In this chapter, information security standards and best practices are compared based on identified criteria by using AHP method. This part is composed by several topics. These topics are the purpose and content of the research, methodology, data collection, steps of the implementation and pair-wise comparisons and the results.

5.1. THE PURPOSE OF THE RESEARCH

Organizations are facing number of problems while providing the security of information. There is always a need for a set of standards to ensure that an appropriate level of security is achieved, the assets and resources are managed efficiently, and the best security applications are applied (An Overview of Information Security Standards, 2008). Best practice frameworks help organizations on defining the security risks, using appropriate security controls, and following the privacy and information security regulations (Saint-Germain, 2005, pg. 60). There are several standards and best practices to provide information security of organizations. In this study the most widely used ones that are applied for information security are selected as a preferential basis. These standards are COBIT, ITIL and ISO 27001 which are used worldwide to provide information security.

Information security has a vital role in protecting the assets that an organization holds. It is achieved by implementing a set of appropriate controls. These controls contain policies, procedures, and organization structure and hardware and software security mechanism. Establishing, implementing and monitoring, reviewing and improving the controls are required to determine and follow the changes that occur in the business environment, the security threats, best practices and regulatory requirements. Business objectives should be met and the process should be in line with other processes of the organization (Xiao-yan, Yu-ging and Li-lei, 2011, pgs. 335-336).

The purpose of the study is to analyze the most used information security standards by identifying the common criteria that each standard has and comparing them by using AHP method. For the reason that, there are several standards and best practices to maintain the security of information, the main point is to decide on the standard that should be implemented. If more than one standard will be applied, then the question is “how should they be combined?”. This study is done to investigate these questions.

5.2. THE CONTENT OF THE RESEARCH

Problem modeling, valuation and aggregation of the weights and sensitivity analysis are the key concepts of AHP. The model is composed by the hierarchical structure of the criteria. They enable decision makers to focus on specific criterion and sub-criterion when allocating the weights. Because of the fact that different hierarchical structure can cause a different ranking, it is vital to structure the criteria and sub-criteria properly. The results obtained from pair-wise comparisons for *n* elements are organized into positive reciprocal *nxn* matrix. The consistency is calculated by the formulas mentioned in the previous chapter. The 1-9 Scale of Saaty is used for the comparisons judgments done by the decision maker. Another important characteristic of the method is the priorities (Franek and Kresta, 2014, pgs. 64-173).

The content of the study is listed and directed as follows;

- Determining information, security and information security.
- Investigating information security standards and best practices which take part in the study, i.e., COBIT, ITIL and ISO 27001.
- Identifying decision making and Analytic Hierarchy Process.
- Establishing a hierarchical structure based on AHP model for the objective, criteria and alternatives.

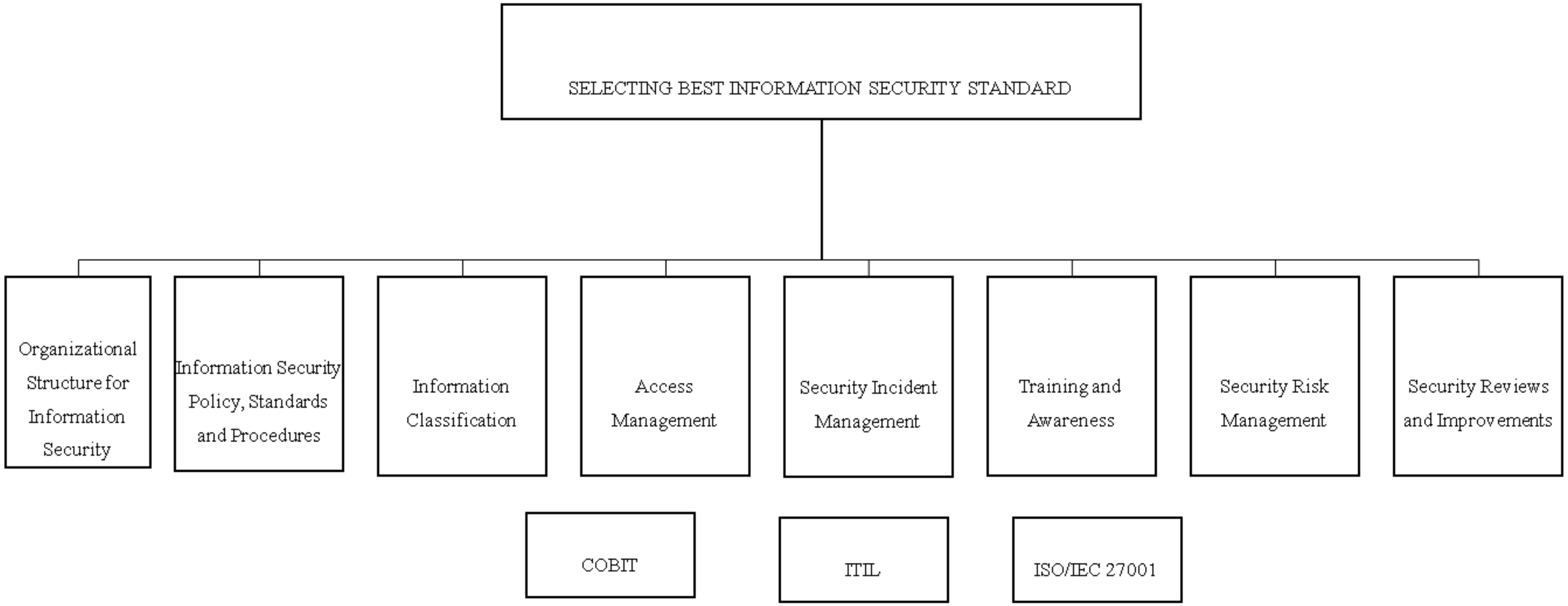
- Accomplishing the pair-wise comparisons by making interview questionnaires with experts and users.
- Computing the inconsistency.
- Obtaining the results and analyzing them.

5.3. DATA COLLECTION

The criteria are selected by identifying the common ones in three alternatives. While making comparisons of criteria and alternatives, an interview questionnaire is done with fifteen experts and users. The experts are chosen from Consulting Agencies and Governmental Institutions who have wide experience and knowledge in the field of Information Technology. Because, information security is very important in the military and banking sector, the users are chosen from the auditors who apply information security standards and best practices in these sectors. Their opinion is also taken to make better judgments. All gathered information helped to define criteria and alternatives and also develop a hierarchical structure.

As a result of the studies done, a hierarchical structure is developed which is shown in Table 5.1.

Table 5.1: The Hierarchical Structure for Selecting the Best Information Security Standard


SELECTING BEST INFORMATION SECURITY STANDARD
Organizational Structure for Information Security
Information Security Policy, Standards and Procedures
Information Classification
Access Management
Security Incident Management
Training and Awareness
Security Risk Management
Security Reviews and Improvements
COBIT
ITIL
ISO/IEC 27001

5.4. STEPS OF THE IMPLEMENTATION

The criteria and alternatives of the research are shown in Table 5.1. There are three alternatives which are COBIT, ITIL and ISO 27001. The area of the study is information security. Because of that, the common criteria of three alternatives in the area of information security are identified.

The criteria that are common in three alternatives are listed as;

- Organizational Structure for Information Security,
- Information Security Policy, Standards and Procedures,
- Information Classification,
- Access Management,
- Security Incident Management,
- Training and Awareness,
- Security Risk Management and
- Security Reviews and Improvements.

Firstly, pair-wise comparisons of all criteria are done one-by-one. At the end of the study, a comparison table is created. Then, a pair-wise comparison of alternatives based on each criterion is done.

5.4.1. Pair-wise Comparisons of Criteria

The arithmetic mean of experts' and users' judgments is taken to calculate the comparison matrixes. After comparing criteria one-by-one, a comparison matrix is created.

Table 5.2: Pair-wise Comparison Matrix for the Criteria

	Organizational Structure for Information Security	Information Security Policy, Stand. & Proc.	Information Classification	Access Management	Security Incident Management	Training and Awareness	Security Risk Management	Security Reviews and Improvements
Organizational Structure for Inform. Security	1	2	4	5	7	6	3	8
Information Security Policy, Stand & Proc.		1	3	4	6	5	2	7
Information Classification			1	2	4	3	1/2	5
Access Management				1	3	2	1/3	4
Security Incident Management					1	1/2	1/5	2
Training and Awareness						1	1/4	3
Security Risk Management							1	5
Security Reviews and Improvements								1

5.4.2. Pair-wise Comparison of Alternatives

Once comparing the criteria one-by-one, it is time to make pair-wise comparisons for alternatives according to each criterion.

Table 5.3: Pair-wise Comparison Matrix for Organizational Structure for Information Security

	COBIT	**ISO 27001**	**ITIL**
COBIT	1	3	7
ISO 27001		1	4
ITIL			1

Table 5.4: Pair-wise Comparison Matrix for Information Security Policy, Standards and Procedures

	COBIT	**ISO 27001**	**ITIL**
COBIT	1	3	9
ISO 27001		1	5
ITIL			1

Table 5.5: Pair-wise Comparison Matrix for Information Classification

	COBIT	**ISO 27001**	**ITIL**
COBIT	1	2	7
ISO 27001		1	5
ITIL			1

Table 5.6: Pair-wise Comparison Matrix for Access Management

	COBIT	**ISO 27001**	**ITIL**
COBIT	1	1/3	4
ISO 27001		1	7
ITIL			1

Table 5.7: Pair-wise Comparison Matrix for Security Incident Management

	COBIT	ISO 27001	ITIL
COBIT	1	3	5
ISO 27001		1	3
ITIL			1

Table 5.8: Pair-wise Comparison Matrix for Training and Awareness

	COBIT	ISO 27001	ITIL
COBIT	1	1/3	3
ISO 27001		1	7
ITIL			1

Table 5.9: Pair-wise Comparison Matrix for Security Risk Management

	COBIT	ISO 27001	ITIL
COBIT	1	3	9
ISO 27001		1	5
ITIL			1

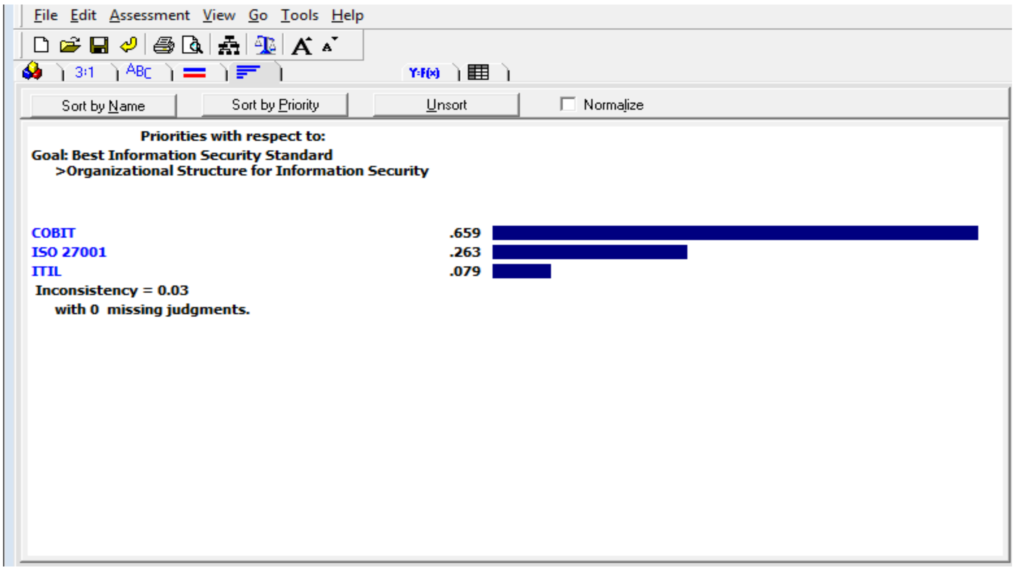
Table 5.10: Pair-wise Comparison Matrix for Security Reviews and Improvements

	COBIT	ISO 27001	ITIL
COBIT	1	2	1/3
ISO 27001		1	1/5
ITIL			1

5.4.3. The Results of Pair-wise Comparisons

The results are obtained by entering all data to Expert Choice Programme. Obtained results are shown in the following tables.

Table 5.11: The result of Expert Choice Programme for Organizational Structure for Information Security



Priorities with respect to:
Goal: Best Information Security Standard
>Organizational Structure for Information Security

COBIT	.659
ISO 27001	.263
ITIL	.079

Inconsistency = 0.03
with 0 missing judgments.

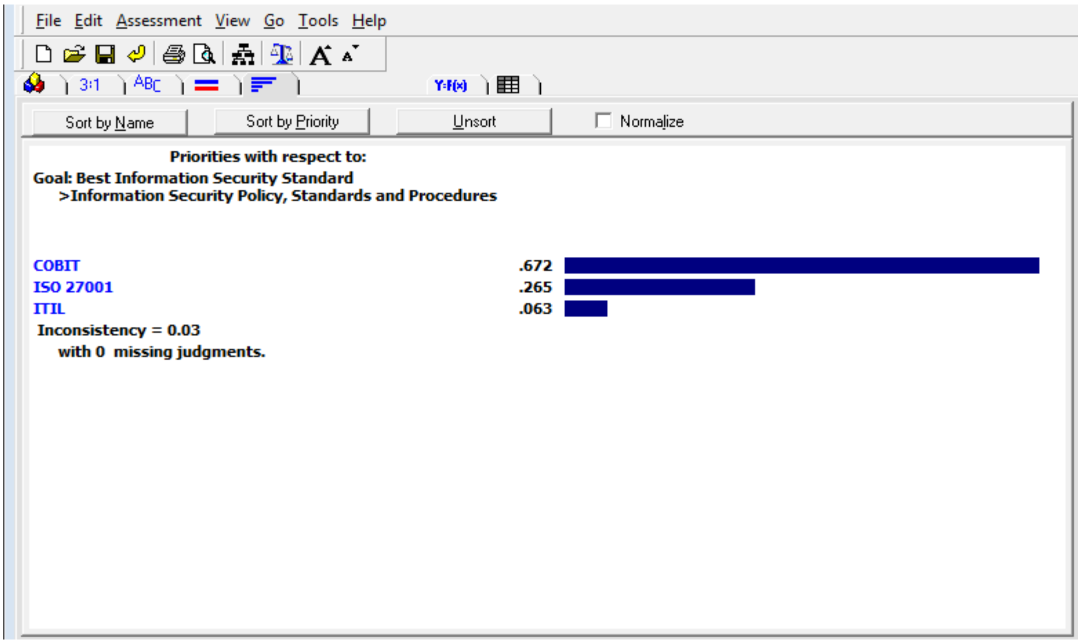
As seen in the Table 5.11, based on Organizational Structure for Information Security criterion, the value of COBIT, ISO 27001 and ITIL is 0.659, 0.263 and 0.079, respectively. There is no missing judgment and inconsistency is 0.03.

According to COBIT, IT security is managed at the highest level. An adequate organizational structure and reporting line for information security exist. There is a security management reporting mechanism which gives information to the board of the organization about the status of information security. A steering committee exists for the areas of key functions. A process is defined to prioritize proposed security initiatives. A charter is established which refers to the organizational risk appetite relative to information security. The charter includes scopes, objectives and responsibilities of the function of security management. Security management function is expected to interact effectively with key functions, including areas such as risk management, compliance and audit. In COBIT, the reporting line of risk management and information security function is expected to be designed and implemented effectively. The roles and responsibilities of security management function have to be formalized and documented.

In ITIL, information security is seen as a management activity within the corporate governance framework. It provides the direction for security activities and makes it possible to achieve established objectives. The information security management process and framework consist of an effective organizational structure. The security manager ensures that technologies, products and services are in place. The manager is also expected to maintain the development of overall policy.

ISO 27001 standard ensures that organizations determine interested parties and their requirements that are related to the information security system. Top management of the organization ensures that information security policy is developed and security objectives are established that are in line with the direction of the organization. Management directs and supports personnel to contribute to the effectiveness of the system. It also allocates responsibility and authority for information security. All employees in the organization are aware of their information security responsibilities.

Table 5.12: The result of Expert Choice Programme for Information Security Policy, Standards and Procedures



Priorities with respect to:
Goal: Best Information Security Standard
>Information Security Policy, Standards and Procedures

COBIT	.672	████████████████████
ISO 27001	.265	████████
ITIL	.063	██

Inconsistency = 0.03
with 0 missing judgments.

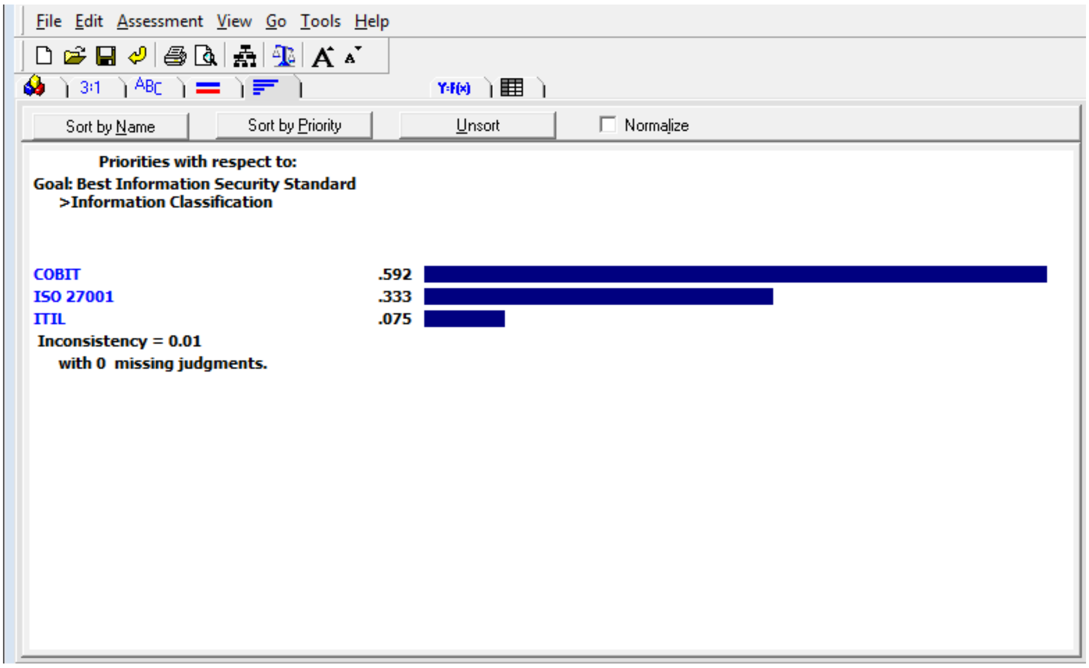
As seen in the Table 5.12, based on Information Security Policy, Standards and Procedures criterion, the value of COBIT, ISO 27001 and ITIL is 0.672, 0.265 and 0.063, respectively. There is no missing judgment and inconsistency is 0.03.

According to COBIT, an information security policy is established. The policy contains the responsibilities of board, executive management, line management, staff members and all users of the enterprise IT infrastructure. IT security plan contains the complete set of security policies and standards in line with the established information security policy framework. Policies, standards and procedures include security compliance policy, management risk acceptance, external communications security policy, firewall policy, e-mail security policy, an agreement to comply with information security policies, laptop/desktop computer security policy and internet usage policy. IT security plan focuses on IT tactical plans, data classification, technology standards, security and control policies, risk management and external compliance requirements. IT contains security policies and standards that are compatible with the information security policy framework, roles and responsibilities, staffing requirements, security awareness and training, enforcement practices and investments in required security sources. The plan is updated on a regular basis.

ITIL defines the purpose of the Information Security Management as to provide a focus for all aspects of IT security and manage all security activities. An Information Security Policy is developed that contains the use and misuse of all IT systems and services. Information security policy is maintained and enforced that fulfills the needs of business security policy and the requirements of corporate governance. The Information Security Management process and framework are composed by Information Security Policy and specific security policies. The policy contains all areas of security and includes several policies such as an overall Information Security Policy, use and misuse of IT assets policy, an access control policy, a password control policy, an e-mail policy, an internet policy, an anti-virus policy, an information classification policy, a document classification policy, a remote access policy, a policy with regard to supplier access of IT service, information and components and an asset disposal policy.

ISO 27001 standard ensures that the information security policy and the information security objectives are established and comply with the strategic direction of the organization. Top management of the organization establishes an information security which is line with the objective of the organization. The information security policy is available as documented information for interested parties and communicated within the organization. The information security objectives are in line information security policy. A set of policies for information are defined and approved by top management of the organization. They are communicated to all interested parties. Information security requirements for mitigating the risks related to supplier's access to the assets are agreed with the supplier.

Table 5.13: The result of Expert Choice Programme for Information Classification



Priorities with respect to:
Goal: Best Information Security Standard
>Information Classification

COBIT	.592	
ISO 27001	.333	
ITIL	.075	

Inconsistency = 0.01
with 0 missing judgments.

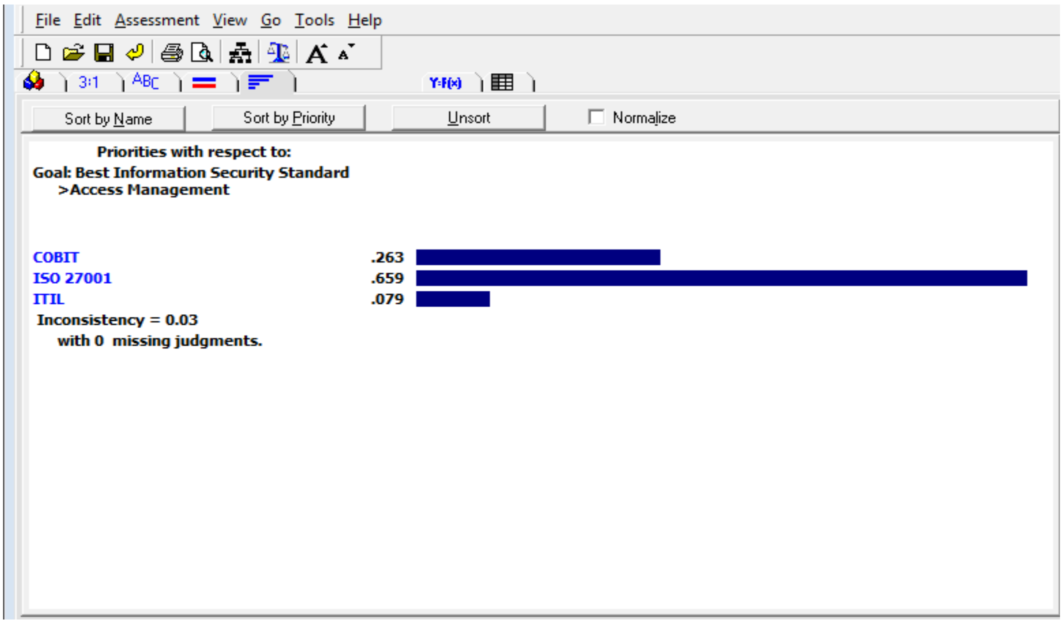
As seen in the Table 5.13, based on Information Classification criterion, the value of COBIT, ISO 27001 and ITIL is 0.592, 0.333 and 0.075, respectively. There is no missing judgment and inconsistency is 0.01.

In COBIT, the organization implements information classification and associated protective controls for information. Information is classified according to the criteria defined by the top management. An information classification scheme is developed. Procedures are established to provide information labeling and handling that are in line with the organization's information classification scheme.

In ITIL, information and repositories are classified according to the sensitivity and the impact of disclosure. The Information Security Policy contains all areas of security and includes an Information Classification Policy.

According to the ISO 27001 standard, the objective of Information Classification is to ensure that information receives an appropriate level of protection in compliance with its importance to the organization. Information is classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. Procedures for information labeling and handling assets are established and applied in compliance with the information classification scheme.

Table 5.14: The result of Expert Choice Programme for Access Management



Priorities with respect to:
Goal: Best Information Security Standard
>Access Management

COBIT	.263	
ISO 27001	.659	
ITIL	.079	

Inconsistency = 0.03
with 0 missing judgments.

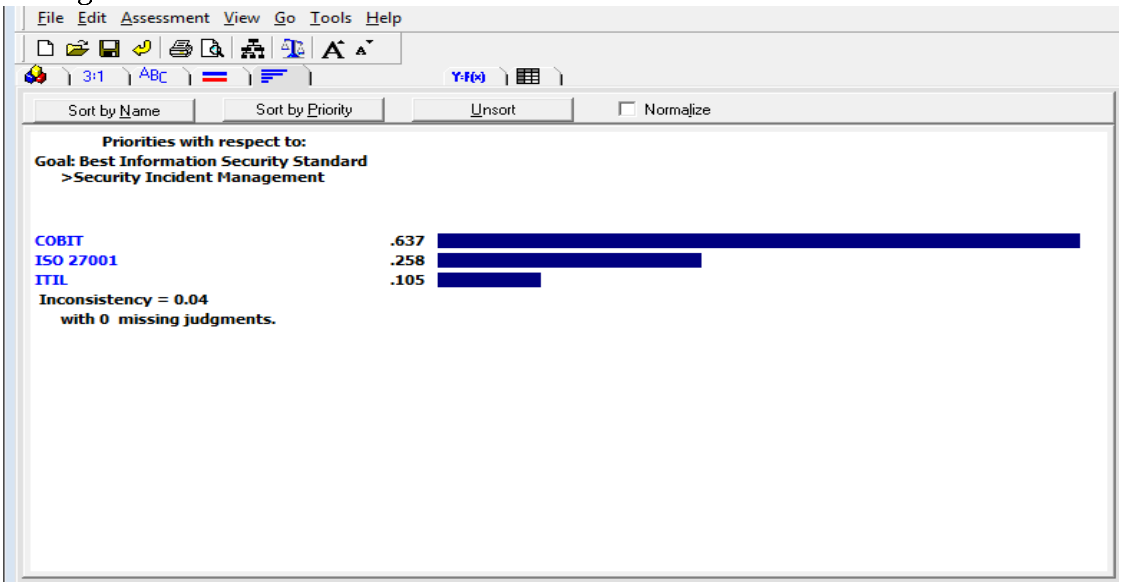
As seen in the Table 5.14, based on Access Management criterion, the value of COBIT, ISO 27001 and ITIL is 0.263, 0.659 and 0.079, respectively. There is no missing judgment and inconsistency is 0.03.

COBIT ensures that all users and their activity on the system are uniquely identifiable. User access rights to systems and data are compatible with defined and documented business needs. Access provisioning and authentication control mechanisms are utilized for controlling logical access. Access control procedures control and manage system and application rights and privileges according to the organization’s security policies and compliance and regulatory requirements. Policies and procedures address security breach consequences. Records are inspected for granting and approving access and logging unsuccessful attempts, lockouts, authorized access to sensitive files and/or data, and physical access to facilities. Access is authorized and appropriately approved.

In ITIL, the information security management contains a set of controls which manage risks associated with access to services, information and systems. The Information Security Policy contains an Access Control Policy, a Remote Access Policy and a policy with regard to supplier access of IT service, information and components. Control of access rights, authorization, identification and authentication and access control are other vital measures. Information Security Management process contains the policies, processes and procedures for managing partners and suppliers and their access to services and information.

According to ISO 27001, the objective of access control is to limit access to information. A policy and supporting security measures are implemented in order to protect information accessed, processed or stored. The allocation and use of privileged access rights are restricted and controlled by a formal management process. Access to information and application system functions are limited in direction with the access control policy. Password management systems are interactive and provide quality passwords. Secure areas are protected properly to prevent from unauthorized access. Physical security for facilities and physical protection against natural disasters, malicious attack or accidents are implemented. Procedures for working in secure areas are established and implemented. Equipment are placed and protected to reduce any risks that may occur.

Table 5.15: The result of Expert Choice Programme for Security Incident Management



Priorities with respect to:
Goal: Best Information Security Standard
>Security Incident Management

COBIT .637
ISO 27001 .258
ITIL .105
Inconsistency = 0.04
with 0 missing judgments.

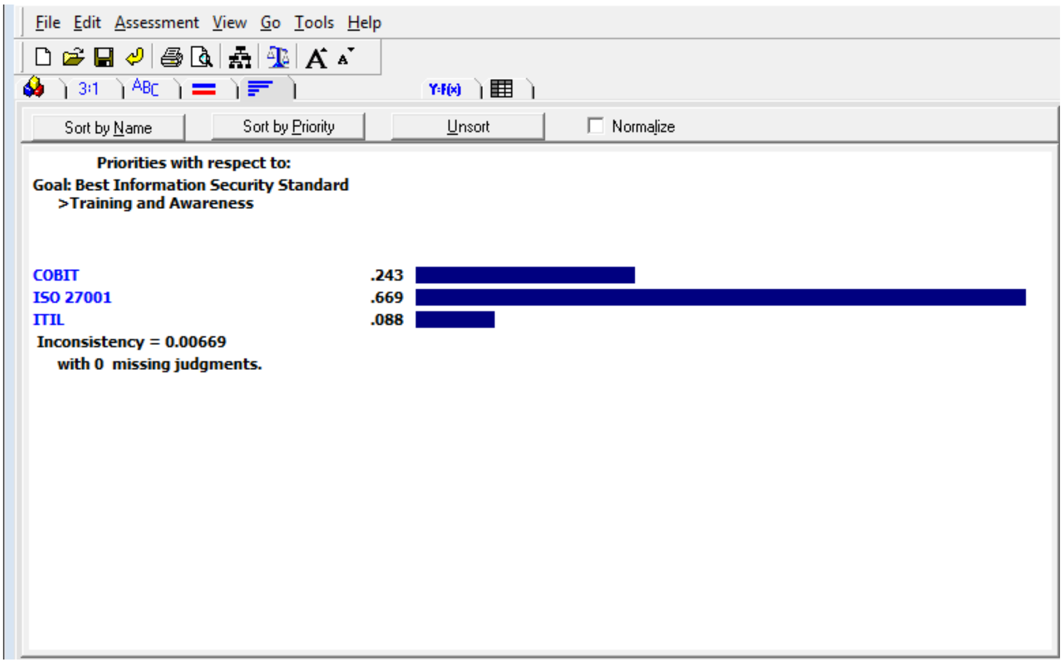
As seen in the Table 5.15, based on Security Incident Management criterion, the value of COBIT, ISO 27001 and ITIL is 0.637, 0.258 and 0.105, respectively. There is no missing judgment and inconsistency is 0.04.

In COBIT, security management contains performing security monitoring, periodic testing and implementing corrective actions for identified security weaknesses. All potential security incidents are defined and communicated. These incidents are classified and treated by the incident and problem management process. A computer emergency response team (CERT) exists. CERT deals with incident handling, vendor relations and communication among key members of management, legal and criminal investigative issues during an incident. According to COBIT, security incident management process interfaces with key organization functions, such as help desk, external service providers and network management. Process of security incident management contains event detection, correlation of events and evaluation of threat/incident, resolution of threat, or creation and escalation work order, criteria for initiating the organization’s CERT process, verification and required levels of documentation of the resolution, post-remediation analysis and work order/incident closure.

Incident and Problem Management is an important part of ITIL. The management provides assistance with the resolution and subsequent justification and correction of security incidents and problems. It includes the ability to define and deal with security incidents. The members of Service Desk and Service Operations recognize and handle security incidents. The information security management contains the management of all security breaches and incidents related to its systems and services. One of the vital activities of information security management process is to monitor and management of security events and incidents. They are analyzed, evaluated and reported properly. If there is an important security incident, it is vital to evaluate the reasons and correct them in order to prevent them in the future. A reporting procedure for security incidents are established to evaluate the effectiveness of the present security measures based on incidents. Recording the incidents is the function of Service Desk.

ISO 27001 defines the objective of information security incident management as ensuring a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. According to standard, the responsibilities of management and procedures are established to provide a quick, effective and orderly response to information security incidents. Information security events are evaluated and decided whether they should be classified as information security incidents or not. Information security incidents are responded according to the documented procedures. Knowledge gained from information security incidents are used to avoid from incidents that may occur in the future.

Table 5.16: The result of Expert Choice Programme for Training & Awareness



Priorities with respect to:
Goal: Best Information Security Standard
>Training and Awareness

COBIT	.243
ISO 27001	.669
ITIL	.088

Inconsistency = 0.00669
with 0 missing judgments.

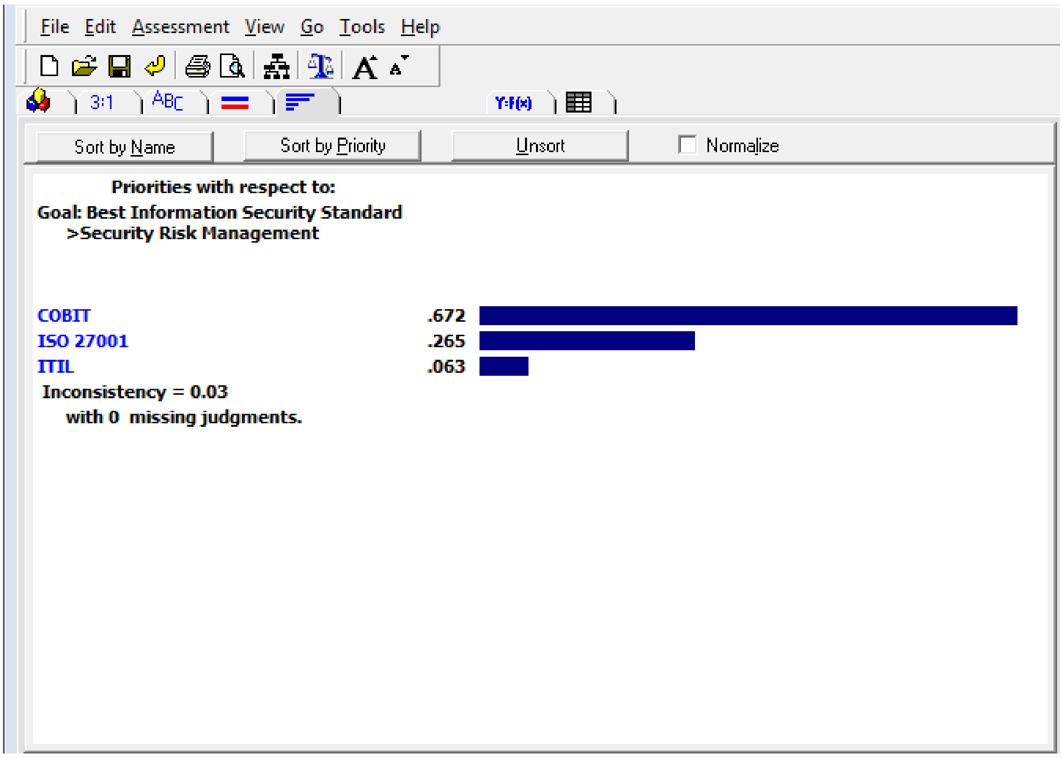
As seen in the Table 5.16, based on Training and Awareness criterion, the value of COBIT, ISO 27001 and ITIL is 0.243, 0.669 and 0.088, respectively. There is no missing judgment and inconsistency is 0.006.

According to COBIT, IT security plan contains security awareness and training. Awareness programs are developed to create and maintain awareness of security in the handling and processing of sensitive data. Regular physical security awareness training is conducted for employees. Security personnel attend annual training. Employee training records are reviewed to evaluate if employees are provided with needed policies and procedures. Content of the program is reviewed to decide whether all internal control frameworks and security requirements are included or not.

The Information Security Management process and framework of ITIL consist of training and awareness strategy and plan. Training and awareness are vital in the overall strategy. One of the main functions of information security management process is to ensure awareness of the security policies amongst the customer community. Increased awareness of the security policy and its contents, throughout the organization is essential for the personnel. Promoting education and awareness of security is included in the tasks and responsibilities of the security manager.

ISO 27001 Standard ensures that personnel of the organization are competent on the basis of appropriate education, training, or experience. All needed parties of the organization receive appropriate awareness education and training. Regular updates on organizational policies and procedures are done.

Table 5.17: The result of Expert Choice Programme for Security Risk Management



Priorities with respect to:
Goal: Best Information Security Standard
>Security Risk Management

COBIT	.672	████████████
ISO 27001	.265	█████
ITIL	.063	█

Inconsistency = 0.03
with 0 missing judgments.

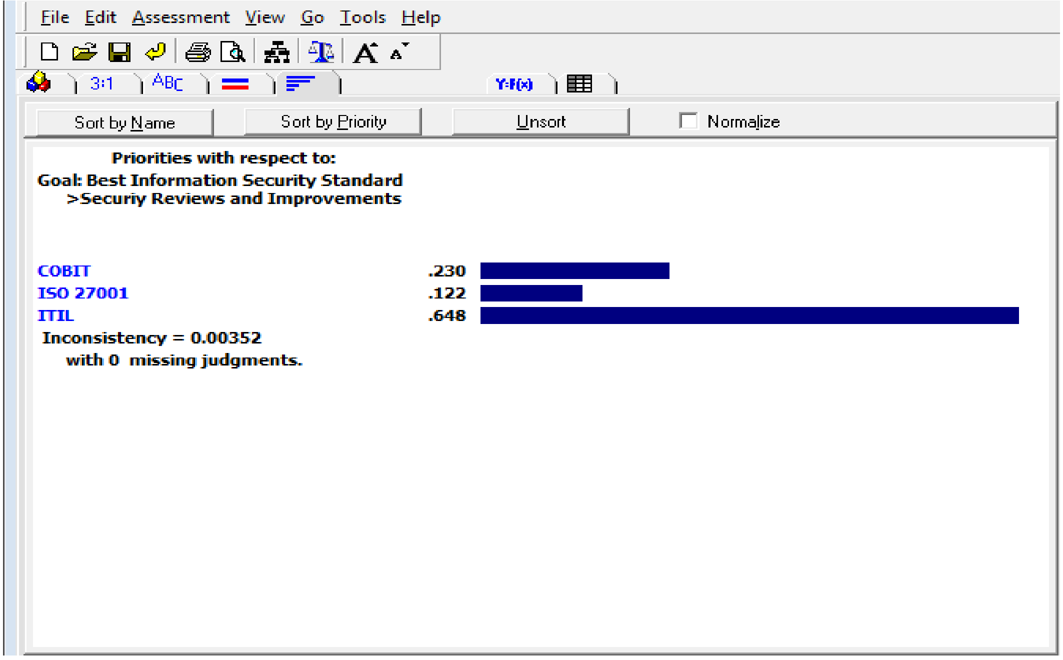
As seen in the Table 5.17, based on Security Risk Management criterion, the value of COBIT, ISO 27001 and ITIL is 0.672, 0,265 and 0.063, respectively. There is no missing judgment and inconsistency is 0.03.

In COBIT, the information security charter includes compliance and risk drivers. Business risk and compliance requirements are translated into an overall security plan. IT security plan considers risk management. Systems, applications and data are classified by levels of importance and risk. All organization-critical, higher-risk network assets are reviewed for security events on regular basis. IT security management function is integrated within the organization's project management initiatives to minimize the risk of new/existing systems introducing security vulnerabilities. CERT process contains the development of a model that identifies the threats and risks to enable focus on risk reduction activities. Security management function effectively interacts with risk management. DS5 of COBIT is about Ensuring Systems Security in which there are eleven control objectives. In each control objective, there are several controls. Security controls are implemented to prevent exposure from malicious attacks and vulnerabilities.

As defined in ITIL, information security is a management activity ensures that the risks of information security are managed effectively. Information security management needs to understand the IT risks. The process of information security management manages risks associated with access to services, information and systems. One of the key activities within the information security management process is to implementation, review, revision and improvement of a set of security controls and risk assessment and responses.

The information security management system of ISO 27001 preserves the confidentiality, integrity and availability of information by applying a risk management process. According to ISO 27001, the organization establishes and implements a documented information security risk assessment process. This process is defined and implemented to select appropriate information security risk treatment options, define all controls that are necessary to implement the chosen information security risk treatment options, develop an information security risk treatment plan, get the approves of risk owners' on it and acceptance of the residual information security risks. The organization has a documented information security risk treatment process and it applies an information security risk treatment plan.

Table 5.18: The result of Expert Choice Programme for Security Reviews and Improvements



Priorities with respect to:
Goal: Best Information Security Standard
>Securiy Reviews and Improvements

COBIT	.230
ISO 27001	.122
ITIL	.648

Inconsistency = 0.00352
with 0 missing judgments.

As seen in the Table 5.18, based on Security Reviews and Improvements criterion, the value of COBIT, ISO 27001 and ITIL is 0.230, 0.122 and 0.648, respectively. There is no missing judgment and inconsistency is 0.003.

In COBIT, a process is defined to periodically update the IT security plan, levels of management review and approval of changes. IT security strategy, plans, policies and procedures that are related to the organization's current IT are updated regularly. Security review process is established and integrated into the organization's processes. User management periodically reviews user profiles and access rights to ensure the adequacy of access rights and requirements for segregation of duties.

In ITIL, there are several policies which are covered by information security policy. All security policies are reviewed and revised. Key activities within the information security management process are reviewed. Revision of policies, security controls, risk assessment, responses, scheduling and completion of security reviews, audits and penetration tests are done. The outputs produced by the

Information Security Management process include reviews and reports of security incidents.

As explained in ISO 27001, top management reviews the organization’s information security management system periodically to ensure its continuing suitability, adequacy and effectiveness. The outputs of the management review contain decisions related to continual improvement opportunities and any needs for changes to the information security management system. The objective of information security reviews is to ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

CHAPTER VI

CONCLUSION

This study focuses on evaluating the information security standards by using Analytic Hierarchy Process. Literature survey has been done to provide detailed information on information security and its standards. Information security is very important for organizations because it ensures the continuous functioning and protection of data created, collected and utilized. Controls and measures can be applied to ensure the effective working of information security within any organization. There are several standards and best practices that provide the security of information such as COBIT, COSO, GAISP, ITIL, ISO 27001, Malcolm Baldridge, PCS DSS and ISF Standard of Good Practice for Information Security. In this study, the most widely used three standards are selected. These standards are COBIT, ITIL and ISO 27001. The study provides a quantitative and qualitative comparison of the alternatives.

There are several studies about information security standards in the literature. Some of these studies deal with the standards particularly whereas some others suggest the integration of different standards. On the other hand, these studies generally don’t indicate the ways to integrate these standards. This study is done to investigate the ways to increase the effectiveness of information security by comparing and then combining the most widely used international information security standards. Unlike other studies, while making comparisons, AHP method is used to determine and evaluate the standards and best practices from the point of information security. In order to evaluate the effectiveness of the standards, the eight criteria that are related to information security are selected. Interview questionnaire is done with experts and users of information security standards to make comparisons of all criteria one-by-one and three alternatives based on each criterion.

The priority of the criteria with their importance value is as below:

– Organizational Structure for Information Security	: 0,332
– Information Security Policy, Standards and Procedures	: 0.231
– Security Risk Management	: 0,155
– Information Classification	: 0,106
– Access Management	: 0,071
– Training and Awareness	: 0,048
– Security Incident Management	: 0,033
– Security Reviews and Improvements	: 0,024

According to this ranking, an organizational structure is established with clear objectives, responsibilities and participation of all related parties. Information security policies, standards and procedures are developed. IT based risks are defined to take actions. By this way, the risks are managed to avoid any adverse impacts that may occur. All information that the organization holds are classified based on its criticality and sensitivity. According to the information classification, access is managed because each employee in the organization has different level of authority to access to information. Employees are trained on a regular basis. Awareness of information security is increased continuously. Security incidents are managed by taking corrective and detective controls. Finally security reviews and improvements on information security system are done regularly.

The result of the study shows that COBIT (0,597) has superiority compare with ISO 27001 (0,315) and ITIL (0,087). If an organization implements COBIT, it can get advantage on establishing an organizational structure for information security, developing information security policies, standards and procedures, managing risks and security incidents and classifying information. By implementing ISO 27001, it is possible to have better management of access to information, well trained employees and increased awareness on information security. ITIL focuses on security improvements.

The controls in COBIT are brought together under a framework. ITIL is issued as a series of five core volumes that are structured as multiple processes communicating each other. On the other hand, the components of ISO 27001 for information security matters are addressed in different standards. In this study, ISO 27001 is selected from among the ISO 27000 series. There are nearly 40 related standards in the series that deal with information security matters. ISO 27001 identifies the requirements for establishing, implementing, maintaining and continuously improving an ISMS. While making interview questionnaires with experts and users, it is proved that ISO 27000 series contain all aspects of information security in different standards. ISO 27001 includes all security matters in brief, whereas other standards of the series approach these matters in detail. This information added a new dimension to the study. Consequently, a new comparison is done. When other standards in ISO 27000 series are taken into account together with ISO 27001, a different result is obtained. According to the pair-wise comparisons, ISO 27000 Series (0,572) has superiority over COBIT (0,323) and ITIL (0,105).

As a result, it is possible to say that there is no standard or best practice that promise hundred percent security success when implemented singly. For that reason, instead of implementing only one standard, combining more than one standard would be for the benefit of the organization. In this study, a road map is determined which combines the three standards. ISO standards are examined in detail from the point of information security. ISO 27001 is the best-known standard of the family. It is strongly advised to implement ISO 27000 series as a whole to establish an effective ISMS. COBIT focuses on what an organization needs to do to have an effective information system security but it does not show the ways to get there. It is process-oriented and control-based. Because of the fact that it explains what to monitor and control, the controls should be done based on COBIT. ITIL can be implemented partially and shows the ways to do things. Therefore, it can be implemented for the areas that need to be improved. Especially, the continual service improvement component of ITIL contains seven steps which increases the efficiency and maximizes the effectiveness of the processes continuously.

The standards that are analyzed in this study are the ones used worldwide. The criteria are selected by identifying the common ones in three alternatives. They cover information security aspect of organizations. The criteria that are not considered in the study could be added to the model or some of the criteria could be removed. This may cause a different result. When there are a high number of criteria and alternatives in the AHP method, the reliability of the analysis may decrease. Because of this, three alternatives and eight criteria are approached in this study. It is difficult to reach people who are specialized in this area and the information they share is critical. Therefore, the interview questionnaire could only conducted to 15 expert and users. The participants of questionnaire are selected mostly from military and banking sectors. The questionnaire would cover more participants from different sectors. This may lead to more sufficient results.

Main approach of this study is to compare the most widely used information security standards to establish a road map in order to increase the efficiency by combining them. A further study may be implemented to extend the model and apply in the other parts of security standards.

CURRICULUM VITAE

PERSONAL INFORMATION

Name - Surname	**: Nurcan TATAR**
Nationality	**:** Turkish
Date of Birth	**:** 10 June 1986 / Manisa
Marital Status	**:** Married
E-mail	**:** nurcanturkol@gmail.com

EDUCATION

Degree	**Institution**	**Year of Graduation**
MBA	Cankaya University Master of Business Administration	2015
BS	Çankaya University, Ankara Faculty of Economics and Administrative Sciences Department of Management (Scholarship)	2009
BS	Avans University of Applied Sciences, Breda / the Netherlands International Business and Management Studies	2008

WORK EXPERIENCE

09/2011-…	İLBANK INC. (Specialist)
08/2011-09/2011	Turkish Electricity Transmission Company
09/2010-08/2011	Vakıfbank INC. (Assistant Specialist)
01/2008-08/2008	Supertape BV, Etten-leur / Hollanda

- Foreign Language : English (KPDS-89)

REFERENCES

Anderson, D. R., Sweeney, D. J. and Williams, T. A. (2005), An Introduction to Management Science: Quantitative Approaches to Decision Making, 11th Edition, Thomson Learning, South-Western.

Arraj, V. (2013), ITIL®: the basics, Compliance Process Partners LLC, White Paper.

Aruldoss, M., Lakshmi, T. M. and Venkatesan, V. P. (2013). A Survey on Multi Criteria Decision Making Methods and Its Applications, *American Journal of Information Systems,* Volume 1, No 1, 31-43.

Baars, H., Hintzbergen, J., Hintzbergen, K., Smulders, A. (2010). *Foundations of Information Security Based on ISO27001 and ISO27002*, Second edition, Van Haren Publishing, the Netherlands.

Dağdeviren, M. and Eren, T. (2001). *Analytical Hierarchy Process and Use of 0-1 Goal Programming Methods in Selecting Supplier Firm,* Gazi University J. Fac. Eng. Arch., Volume 16, No 2, 41-52.

Dağdeviren, M., Akay, D. and Kurt, M. (2004). Analytical Hierarchy Process for Job Evaluation and Application, *Gazi University J. Fac. Eng. Arch.,* Volume 19, No 2, 131-138.

Disterer, G. (2013), ISO/IEC 27000, 27001 and 27002 for Information Security Management, *Journal of Information Security*, Volume 4, No 2, 92-100.

Duffy, N. M. and Assad, M. G. (1980). *Information management: an executive approach.* Oxford University Press, USA.

Farradane, J. (1979). The Nature of Information, *Journal of Information Science,* Volume 1, No 1, 13-17.

Franek, J., and Kresta, A., Judgment Scales and Consistency Measure in AHP, Procedia Economics and Finance, Enterprise and the Competitive Environment 2014 Conference, ECE 2014, 6–7 March 2014, Brno Czech Republic, 164-173.

Gehrmann, M. (2012), Combining ITIL, COBIT and ISO/IEC 27002 for Structuring Comprehensive IT for Management in Organizations, *Navus- Revista de Gestao e Tecnologia*, 66-76.

Green C. W., Hurley, T. and Shaw, P. (2004). *Knowledge management in organizational settings: The Effect of Normative Influence and Technological Support on Knowledge Creation and Transfer*. Proceedings on 2004 Information Resources Management Association International Conference, New Orleans, LA (444-446). Hershey, PA: Idea Group Publishing.

Hansche, S., Berti, J. and Hare, C. (2003). *Official (ISC2) Guide to the CISSP Exam*, Auerbach Publication.

Ho, S.M**.**, and Wang, C. (2005) Security-Based Knowledge Management. In M. Khosrow-Pour (Ed.), E*ncyclopedia of Information Science and Technology*, 2nd Ed. (3401-3405). Hershey, PA: Information Science Reference.

Ho, W. (2008). Integrated Analytic Hierarchy Process and Its Applications, *European Journal of Operational Research*, 211-228.

http://www.infosec.gov.hk/english/technical/files/overview.pdf, An Overview of Information Security Standards (2008), The Government of the Hong Kong Special Administrative Region, Accessed: 04.12.2014.

http://www.umassd.edu/media/umassdartmouth/fycm/Decision_making_process.pdf Decision-Making Process. Accessed: 10.11.2014

http://www.utica.edu/faculty_staff/qma/needforsecurity.pdf , The Need for Security, Accessed: 18.10.2014.

http://www.merriam-webster.com/dictionary/security , Accessed: 19.09.2014.

http://www.writeopinions.com/parkerian-hexad, the Parkerian Hexad Model. Accessed: 23.09.2014.

Hummel, J. M. (2001). *Supporting Medical Technology Development with the Analytic Hierarchy Process*, Printed by Grafisch bedrijf Ponsen and Looijen BV, the Netherlands.

Information Security Standards, http://www.iso27001security.com/. Accessed: 14.01.2015.

Ishizaka, A. (2004). Advantage of Clusters and Pivots in AHP, Proceedings of the 15th Mini-Euro Conference, Portugal.

ISO/IEC 27001:2013 Information Technology – Security techniques – Information Security Management Systems – Requirements, 2013, Second Edition, published in Switzerland.

ISO/IEC 27035:2011 Standard, Information Technology — Security techniques — Information Security Incident Management.

Jones, G.R. and George, J.M. (2003). *Contemporary Management*, Third Edition, McGraw-Hill Company, New York.

Koçel, T. (2003). *İşletme Yöneticiliği*, 9th Edition, Beta Publish, İstanbul.

Lai, V. S., Wong, B. K. and Cheung, W. (2002). Group Decision Making in a Multiple Criteria Environment: A case using the AHP in a software selection, *European Journal of Operational Research*, 137, 134-144.

Lunenburg, F.C. (2010). The Decision Making Process, *National Forum of Educational Administration and Supervision Journal*, Vol. 27, No. 4, 1-12. http://www.nationalforum.com/Electronic%20Journal%20Volumes/Lunenburg,%20Fred%20C.%20The%20Decision%20Making%20Process%20NFEASJ%20V27%20N4%202010.pdf . Accessed: 18.11.2014.

Malone, T., Menken, I., Blokdijk, G. (2009), ITIL V3 Foundation Complete Certificate Kit: Study Guide Book and Online Course, the Art of Service Pty Ltd, 2009 Edition.

Marquis, H. (2006), ITIL: What It Is and What It Isn’t, Business Communications Review, December 2006, 49-52.

Mataracıoğlu, T. and Ozkan, S. (2011), Governing Information Security in Conjunction with COBIT and ISO 27001, *International Journal of Network Security and Its Applications,* Vol. 3, No. 4, 111-115.

Mathew, N. and Basel, A. M. (2012), Success Factors for Integrated ITIL Deployment: An IT Governance Classification, *Journal of Information Technology Case & Application Research*, Vol. 14, No. 1, 25-54.

Mescon, H. M., Bovee C. L. and Thill, J. V. (2002). *Business Today*, Tenth Edition, Prentice Hall. Bovee&Thill LLC.

National Institute of Standards and Technology. (2004), *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Procesing Standards Publication, FIPS Publication 199, Gaithersburg.

Pena, J., Vicente, E. and Ocana, A. (2013), ITIL, COBIT and EFQM: Can They Work Together?, *International Journal of Combinatorial Optimization Problems and Informatics,* Vol. 4, No. 1, 54-64.

PowerTech, COBIT (2010), http://www.powertech.com/guides/Compliance/cobit.htm Accessed: 25.10.2014.

Saaty, T. L. (1977). A Scaling Method for Priorities in Hierarchical Structures, *Journal of Mathematical Psychology*, Vol. 15, No. 3, 234-281.

Saaty, T.L. (1980). The Analytic Hierarchy Process. McGraw-Hill International, New York, U.S.A.

Saaty, T. L. (1994). *How to Make a Decision: The Analytic Hierarchy Process,* The Institute of Management Sciences, Interfaces 24: 6, 19-43.

Saaty, T. L. (1997). That is not the Analytic Hierarchy Process: What the AHP Is and What It Is Not. *Journal of Multi-Criteria Decision Analysis*. Vol. 6, No. 6, 324-335.

Saaty, T. (2008). Decision Making with the Analytic Hierarchy Process. *International Journal of Services Sciences*, 83-98.

Saint-Germain, R.(2005), Information Security Management Best Practice Based on ISO/IEC 17799, *The Informaiton Management Journal*, 60-66.

Sheikhpour, R. and Modiri, N. (2012a), “An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls”, *International Journal of Security and Its Applications*, Vol. 6, No. 2, 13-27.

Sheikhpour, R. and Modiri, N. (2012b), A Best Practice Approach for Integration of ITIL and ISO/IEC 27001 Services for Information Security Management, *Indian Journal of Science and Technology*, Vol. 5, No. 2, 2170-2176.

Subaşı, H. (2011). Comparison of TOPSIS and AHP Methods in Multi-criteria Decision Process and an Application, Master Thesis, Marmara University Social Sciences Intuition, Istanbul.

Susanto, H., Almunawar, M. N., Tuan, Y. C. (2011), Information Security Management System Standards: A Comparative Study of the Big Five, *International Journal of Electrical and Computer Sciences IJECS-IJENS*, Vol. 11, No. 5, 21-27.

Tanuwijaya, H. and Sarno, R. (2010), Comparation of CobiT Maturity Model and Structural Equation Model for Measuring the Alignment between University Academic Regulations and Information Technology Goals, *IJCSNS International Journal of Computer Science and Network Security*, Vol. 10, No. 6, 80-92.

The Stationary Office (2011), ITIL Service Design, the 2011 Edition, the United Kingdom.

The Stationary Office (2011), ITIL Service Transition, the 2011 Edition, the United Kingdom.

The Stationary Office (2011), ITIL Service Operation, the 2011 Edition, the United Kingdom.

The Stationary Office (2011), ITIL Service Strategy, the 2011 Edition, the United Kingdom.

The Stationary Office (2011), ITIL Continual Service Improvement, the 2011 Edition.

The ITIL Service Lifecycle, http://www.best-management-practice.com/serviceOperation2011_demo/ , Accessed: 02.11.2014.

The IT Governance Institute (2007), COBIT 4.1 Framework - Control Objectives - Management Guidelines - Maturity Models, The United States of America.

The IT Governance Institute (2007), COBIT Control Practices – Guidance to Achieve Control Objectives for Successful IT Governance, the United States of America.

The IT Governance Institute (2007), COBIT 4.1. Excerpt, the United States of America.

The IT Governance Institute (2007), IT Assurance Guide – Using COBIT, the United States of America.

The UK Chapter of the itSMF Ltd (2012), An Introductory Overview of ITIL V3 2011, Published by the Stationery Office.

Triantaphyllou, E. and Mann, S. H. (1995). Using the Analytic Hierarchy Process for Decision Making in Engineering Applications: Some Challenges, *International Journal of Industrial Engineering*, Vol. 2, No. 1, 35-44.

UCISA ITIL: A Guide to Service Asset and Configuration Management: https://www.ucisa.ac.uk/~/media/Files/members/activities/ITIL/servicetransition/service_asset/ITIL_guide%20to%20SA%20and%20CM%20management%20pdf.ashx , Accessed: 24.10.2014.

Velasquez, M. and Hester, P. (2013), An Analysis of Multi-criteria Decision Making Methods, *International Journal of Operations Research*, Vol. 10, No. 2, 56-66.

Wind, Y. and Saaty, T. L. (1980). Marketing Application of the Analytic Hierarchy Process, *Management Science*, Vol. 26, No. 7, 641-658.

Withman, M. H. and Mattord, H. J. (2011). *Principles of information security*, 4th edition, Cengage Learning. USA.

Xiao-yan, G., Yu-ging, Y., and Li-lei, L. (2011), An Information Security Maturity Evaluation Mode, 2011 International Conference on Advances in Engineering, 2011, 335-339.

Yates, J. F., Veinott, E. S., and Patalano, A. L. (2003). *Hard decisions, Bad decisions: On Decision Quality and Decision Aiding*. Schneider, S. L. and Shanteau, J. C. (Eds.), Emerging Perspectives on Judgment and Decision Research. New York, Cambridge University Press.

APPENDIX I: EXPERT/USER EVALUATION QUESTIONNAIRE FOR PAIR-WISE COMPARISON OF CRITERIA

Please compare the importance of two criteria, according to their effects on Information Security																		
Organization Structure for Information Security	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Information Security Policy, Standard & Procedures**
Organization Structure for Information Security	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Information Classification**
Organization Structure for Information Security	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Access Management**
Organization Structure for Information Security	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Security Incident Management**
Organization Structure for Information Security	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Training and Awareness**
Organization Structure for Information Security	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Security Risk Management**
Organization Structure for Information Security	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Security Reviews and Improvements**
Information Security Policy, Standard & Procedures	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Organization Structure for Information Security**
Information Security Policy, Standard & Procedures	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Information Classification**
Information Security Policy, Standard & Procedures	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Access Management**

APPENDIX I (CONT.) EXPERT/USER EVALUATION QUESTIONNAIRE FOR PAIR-WISE COMPARISON OF CRITERIA

Information Security Policy, Standard & Procedures	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	**Security Incident Management**
Information Security Policy, Standard & Procedures	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	**Training and Awareness**
Information Security Policy, Standard & Procedures	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	**Security Risk Management**
Information Security Policy, Standard & Procedures	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	**Security Reviews and Improvements**
Information Classification	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	**Organization Structure for Information Security**
Information Classification	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	**Information Security Policy, Standard & Procedures**
Information Classification	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	**Access Management**
Information Classification	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	**Security Incident Management**
Information Classification	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	**Training and Awareness**
Information Classification	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	**Security Risk Management**
Information Classification	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	**Security Reviews and Improvements**

APPENDIX I (CONT.) EXPERT/USER EVALUATION QUESTIONNAIRE FOR PAIR-WISE COMPARISON OF CRITERIA

Access Management	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Information Security Policy, Standard & Procedures**
Access Management	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Organization Structure for Information Security**
Access Management	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Information Classification**
Access Management	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Security Incident Management**
Access Management	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Training and Awareness**
Access Management	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Security Risk Management**
Access Management	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Security Reviews and Improvements**
Security Incident Management	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Information Security Policy, Standard & Procedures**
Security Incident Management	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Organization Structure for Information Security**
Security Incident Management	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Information Classification**
Security Incident Management	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Access Management**

APPENDIX I (CONT.) EXPERT/USER EVALUATION QUESTIONNAIRE FOR PAIR-WISE COMPARISON OF CRITERIA

Security Incident Management	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Training and Awareness
Security Incident Management	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Security Risk Management
Security Incident Management	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Security Reviews and Improvements
Training and Awareness	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Information Security Policy, Standard & Procedures
Training and Awareness	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Organization Structure for Information Security
Training and Awareness	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Information Classification
Training and Awareness	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Access Management
Training and Awareness	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Security Incident Management
Training and Awareness	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Security Risk Management
Training and Awareness	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Security Reviews and Improvements
Security Risk Management	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	Information Security Policy, Standard & Procedures

APPENDIX I (CONT.) EXPERT/USER EVALUATION QUESTIONNAIRE FOR PAIR-WISE COMPARISON OF CRITERIA

Security Risk Management	**9**	**8**	7	**6**	5	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Organization Structure for Information Security**
Security Risk Management	**9**	**8**	7	**6**	5	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Information Classification**
Security Risk Management	**9**	**8**	7	**6**	5	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Access Management**
Security Risk Management	**9**	**8**	7	**6**	5	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Security Incident Management**
Security Risk Management	**9**	**8**	7	**6**	5	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Training and Awareness**
Security Risk Management	**9**	**8**	7	**6**	5	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Security Reviews and Improvements**
Security Reviews and Improvements	**9**	**8**	7	**6**	5	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Information Security Policy, Standard & Procedures**
Security Reviews and Improvements	**9**	**8**	7	**6**	5	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Organization Structure for Information Security**
Security Reviews and Improvements	**9**	**8**	7	**6**	5	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Information Classification**
Security Reviews and Improvements	**9**	**8**	7	**6**	5	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Access Management**
Security Reviews and Improvements	**9**	**8**	7	**6**	5	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Security Incident Management**
Security Reviews and Improvements	**9**	**8**	7	**6**	5	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Training and Awareness**

APPENDIX I (CONT.) EXPERT/USER EVALUATION QUESTIONNAIRE FOR PAIR-WISE COMPARISON OF CRITERIA

Security Reviews and Improvements	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Security Risk Management**

APPENDIX II: EXPERT/USER EVALUATION QUESTIONNAIRE FOR PAIR-WISE COMPARISON OF ALTERNATIVES

<table>
<tr><th colspan="19">Please compare two alternatives according to their importance on
“<i>Organizational Structure for Information Security</i>”</th></tr>
<tr><td>COBIT</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>ITIL</td></tr>
<tr><td>COBIT</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>ISO27001</td></tr>
<tr><td>ITIL</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>ISO27001</td></tr>
</table>

<table>
<tr><th colspan="19">Please compare two alternatives according to their importance on
“<i>Information Security Policy, Standards and Procedures</i>”</th></tr>
<tr><td>COBIT</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>ITIL</td></tr>
<tr><td>COBIT</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>ISO27001</td></tr>
<tr><td>ITIL</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>ISO27001</td></tr>
</table>

<table>
<tr><th colspan="19">Please compare two alternatives according to their importance on
<i>“Information Classification”</i></th></tr>
<tr><td>COBIT</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>ITIL</td></tr>
<tr><td>COBIT</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>ISO27001</td></tr>
<tr><td>ITIL</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>ISO27001</td></tr>
</table>

<table>
<tr><th colspan="19">Please compare two alternatives according to their importance on
<i>“Access Management”</i></th></tr>
<tr><td>COBIT</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>ITIL</td></tr>
<tr><td>COBIT</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>ISO27001</td></tr>
<tr><td>ITIL</td><td>9</td><td>8</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>ISO27001</td></tr>
</table>

APPENDIX II (CONT.) EXPERT/USER EVALUATION QUESTIONNAIRE FOR PAIR-WISE COMPARISON OF ALTERNATIVES

Please compare two alternatives according to their importance on ***“Security Incident Management”***																	
COBIT	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**ITIL**
COBIT	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**ISO27001**
ITIL	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**ISO27001**

Please compare two alternatives according to their importance on ***“Training and Awareness”***																		
COBIT	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**ITIL**
COBIT	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**ISO27001**
ITIL	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**ISO27001**

Please compare two alternatives according to their importance on ***“Security Risk Management”***																		
COBIT	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**ITIL**
COBIT	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**ISO27001**
ITIL	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**ISO27001**

Please compare two alternatives according to their importance on ***“Security Reviews and Improvements”***																		
COBIT	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**ITIL**
COBIT	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**ISO27001**
ITIL	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**ISO27001**