Requirement Identification for the Development of Information Security Readiness Indicators for the Implementation of E-government in Yemen

By

Jabeir Mohammed Hussein Ahmed Amer

This thesis is submitted in partial fulfilment of the requirements
for the Degree of Doctor of Philosophy in
Information Technology

ST. CLEMENTS UNIVERSITY
BRITISH WEST INDIES

JUNE 2011

Requirement identification for the Development of Information Security Readiness Indicators for the Implementation of E-government in Yemen

By

Jabeir Mohammed Hussein Amer

Supervisor:
Dr. Adnan AL-Sqaf

This thesis is submitted in partial fulfilment of the requirements
for the Degree of Doctor of Philosophy in
Information Technology

ST. CLEMENTS UNIVERSITY
BRITISH WEST INDIES

JUNE 2011

APPROVED:

DR. ADNAN ZEN AL-SQAF, Supervisor and Committee Head.
DR. ABRAHEM ABD AL-RAB, Committee member.
DR. RASHAD AL-GOFI, Committee member.

ABSTRACT

E-government security is considered to be one of the crucial factors for achieving an advanced stage of e-government. Because today's economies depend on the secure flow of information within and across organizations, information security is an issue of vital importance. A secure and trusted environment for stored and shared information greatly enhances consumer benefits, business performance and productivity, and national security.

This thesis provides a new approach for the assessment of security readiness indicators, based on development of a mathematical model. This approach introduces an analytical method for the assessment, which accommodates the various factors considered, both individually and collectively, according to the multi-layer model layers" technology, policy, Operational and management, Competencies, and decision layer". These indicators provide a comprehensive picture of the strengths and the weaknesses of information security in government organizations; and this helps toward security requirement identification and information security improvement for the implementation of e-government. In addition, this thesis is associated with using of the model for the investigation of information security readiness in Yemen government organizations for implementation of e-government .This work would be useful to all organizations concerned with providing E-business. This research will discuss issue of information security in e-government, which will help decision makers and officials on the implementation of e-government in Yemen to overcome some of the problems and challenges that await them in the future during the implementation, and increase citizen’s trust in online transaction and transfer of important personal and

organizational information. And suggests security solutions for e-government security and provide some recommendations in light of results of the survey carried out on many government organizations in Yemen.

الملخص

أمن الحكومة ألالكترونية يُعتَبرُ من أهم العوامل لإنجاز المرحلةَ المتقدّمة مِنْ الحكومة الإلكترونيةِ. فاقتصاديات اليوم تَعتمدُ على انتقال المعلوماتِ بين المؤسسات بشكل امن فأمن المعلوماتِ قضية مهمة وحيوية. فالبيئة الآمنة والموثوقة لتخزين ومشاركة المعلومات تحسن كثيرا من أداء العمل ومعدل الإنتاج وزيادة الأمن الوطني.

هذه الأطروحة تهتم بتُزوّدُ طريقة جديدة لتقييم مؤشراتِ الاستعدادات الأمنية، بالاعتماد على تطوير نموذج رياضي، تُقدّمُ هذه الطريقة أسلوب جديد للتقييم، وفقا لموديل متعدد الطبقات ً "تقنية، سياسة، تنظيميه وإدارية، كفاءة، واتخاد القرار" . هذه المؤشراتِ تُزوّدُ صورة شاملة لعوامل القوة والضعف لأمن المعلوماتِ في المنظمات الحكوميةِ؛ مما يُساعدُ في تحديد المتطلبات الأمنية و تحسين امن المعلومات لتنفيذ الحكومة الإلكترونيةِ.فهذه الأطروحة اهتمت بالتحقق من هذا النموذج بتطبيق وقياس مؤشرات الجاهزية لأمن المعلوماتِ في المظمات الحكوميةِ لتطبيق الحكومة الإلكترونيةِ باليمن. وهذا العمل يفيدَ جميع المظمات المُهتمّة بتطويرالجاهزية الأمنية للمنظمات التي تقدم خدمات الكترونية و الأعمال الالكترونية.

بالإضافة إلى أن هذه الدراسة تناقش القضايا المتعلقة بأمن المعلومات للحكومة الالكترونية والتي تساعد متخذي القرار والمسئولين على تنفيذ مشروع الحكومة الالكترونية باليمن على التغلب على العديد من المشاكل والتحديات التي قد يواجهونها في المستقبل خلال التنفيذ،ويعمل على زيادة الثقة بالتعاملات الالكترونية وانتقال المعلومات المهمة والخاصة بالأشخاص والمنظمات، ويقترح الحلول الأمنية لتامين الحكومة الالكترونية ويزود بالتوصيات على ضوء النتائج التي توصلت إليها الدراسة.

Dedication

I dedicate this work to my mother, to my father for his support and encouragement during the study.

To my sons “Asem and Khalid”, to my daughter Nada, and

To my wife, for her support, patience and for taking care of our sons and daughter during the whole period of the study.

To whom Allah said to them:

(Men who have been true to their covenant with Allah).

Acknowledgement

Firstly, I would like to thank my Allah, and I would like to thank my supervisor, Professor Dr. Adnan al-sqaf for constructive advice and guidance throughout this research work, and to Professor Dr. Abrahim abd-Al-rab and Professor Dr. Rashad AL-Gofi – Committee members.
Secondly, I would like to take this opportunity to thank my University (St. Clements University) and Special thanks to Dr. Ahmed Qutran Dr.and Mohammed AL-Shbatat and Asmail al-Ansi.
Thirdly, my thanks go to Mrs. Sami AL-Faiq for checking the English of this thesis at an early stage.

	Table of Contents	
		Page no.

List of Tables

Chapter One

Introduction

1.1 Introduction

Electronic government, or e-Government, is enabling government organizations to provide with better services to their constituents. Transactions such as filing taxes online, applying for jobs, renewing driver's licenses, and ordering recreational and occupational licenses can now be conducted online, quickly and efficiently.

E-government, the application of Information and Communication Technology within public administration to optimize its internal and external functions, government provides, citizen and business with a set of tools that can potentially transform ways in which interactions take place, services are delivered, knowledge is utilized, developed and implemented policies, citizens participate in governance, and public conceived use of Information and Communication Technology (ICTs) in government administration reform and good governance goals are met strategic and wells also can result in a more inclusive, effective, efficient, transparent, accountable and "people centered" public

administration. Moreover, they can serve as a vehicle for meeting the Millennium development Goals across sectors such as governance, economic development, health, education, the environment and …etc. E-government security is considered one of the crucial factors for achieving an advanced stage of e-government (Power, 2002).E-government has become very important to all countries, developed and developing, because of the strong links between knowledge and productivity, and between competitiveness, and economic growth (World Bank, 2002). The implementation of e-government in Yemen is to improve the efficiency, effectiveness, transparency, and accountability of government. The Yemen is a third world country that is trying to implement e-government not just in its private organizations but also in its governmental agencies. The Yemeni government is trying to find the appropriate e-government framework to enhance the economical growth and provide the people with the best and fastest services offered by this new technology (Alsohybe, 2007).

The work of this thesis is concerned with development of Multi-layer model, and with selecting Yemen government a case-study in order to investigate practical, test validity and increase its usability. This research will discuss issue of information security in e-government, which will help decision makers and officials on the implementation of e-government in Yemen to overcome some of the problems and challenges

that await them in the future during the implementation, and increase citizen's trust in online transaction and transfer of important personal and organizational information. And suggests security solutions for e-government security and provide some recommendations in light of results of the survey carried out on many organizations in Yemen.

1.2 Yemen's Background

Yemen is one of the developing countries which located in the southern part of the Arabian Peninsula. It is bounded on the north by Saudi Arabia and by the Arab Sea. Oman lies in the west of the Republic of Yemen and the Red Sea lies in the west of the Republic of Yemen. The total area of the Republic of Yemen is about 555,000 square Kilometer, and the population of Yemen is 21 million (NIC, 2010). The official language of the country is Arabic and Islam is the official religion of the country. The Yemeni Rial (YR) is the official currency unit. The Republic of Yemen has three national independence days: September 26, 1962 when the king of North the Republic of Yemen, at that time, was overthrown and making the country a republic instead of a kingdom, November 30, 1967 when South the Republic of Yemen, at that time, had become independent from United Kingdom. The Unification Day on May 22, 1990, when the Republic of Yemen was established by the merger of South the Republic of Yemen and North the Republic of Yemen. The

Republic of Yemen is one of the poorest countries in the Arab World. It has reported strong growth since 2000, and its economic fortunes depend mostly on oil. The government represented by the president initiated a plan to develop the new country infrastructure and build a democratic administrative system, which is responsible for the provision of public services to all Yemenis whether in the country or abroad. According to (Alsohybe, 2007) the Republic of Yemen long-term's strategy aimed to develop a reliable and efficient administration and government by improving and reforming its ministries and institutions to deliver better public services for all its citizens and gain recognition around the world. However, not all the goals were aimed at improving the governmental functions were achieved. There are still problems facing the government plan to reform like, inflated bureaucracy, lack of collaboration between ministries and agencies, illiteracy, and a lack of direct vision of the future of the country. In its attempt to overcome these problems, the government of the Republic of Yemen has launched a reform project using information technology to implement e- government in the next couple of Years. The implementation of information technology will lead into collaboration between governmental agencies and lead to integrated databases that can be accessed by any agency any time thus delivering rapid and efficient service to the public.

1.2.1 ICT INFRASTRUCTURE

Yemen is in lowest level of ICT infrastructure in world, this level is characterized by the following: (a) low penetration rates of fixed and mobile telephone lines; (b) lack of an environment conducive to widespread use of telecommunication services by businesses and individuals; and (c) insufficient national bandwidth ,inadequate backbone for voice and data telecommunication and insufficient number of Internet players in the market (ESCWA, 2009). A table 1-1 shows that Yemen country index in term of using computers and Internet, telephone usage.

Table 1-1 Telecommunication infrastructure index and its components in Yemen (*Source :* United Nations E-Government Survey 2010)

country	Index value	Estimated Internet users per 100 inhabitants	Main fixed telephone lines per 100 inhabitants	Mobile subscribers per 100 inhabitants	Personal computers per 100 inhabitants	Total fixed broadband per 100 inhabitants
Yemen	**0.0298**	**1.44**	**4.48**	**13.76**	**2.77**	**0.00**

Table 1-2 compare Yemen to other countries around the world and show that the Yemen is still one of the lowest countries in term of E-government envelopment.

Table 1-2 E-government development for Some Countries Including the Yemen between “2008-2010” (*Source :* United Nations E-Government Survey 2010)

Country	E-government development index value		World e-government development ranking	
	2010	2008	2010	2008
Bahrain	0.7363	0.5723	13	42
United Arab	0.5349	0.6301	49	32
Kuwait	0.5290	0.5202	50	57
Jordan	0.5278	0.5480	51	50
Saudi Arabia	0.5142	0.4935	58	70
Qatar	0.4928	0.5314	62	53
Oman	0.4576	0.4691	82	84
Lebanon	0.4388	0.4840	93	74
Syrian Arab	0.3103	0.3614	133	119
Iraq	0.2996	0.2690	136	151
Yemen	0.2154	0.2142	164	164

1.3 Research Problem

The Multi–layer model was developed by Alazazi in 2008(Alazazi, s., 2008). It is a model for e-government information security assessment, consists of five layers. Each layer represents a dimension of security which needs to be addressed in order to mitigate threats associated with it. It has one or more of sub layers. The number of sub layers will be determined by number of security measures an e-government organization feel sufficient to provide an acceptable security level. The only model reflects the layers and sub layers required to provide an acceptable security program for any e-government organization offering services to the public citizens. The model establishes, the sub layers is the most required for the security program to tackle the multiple threats associated with an e-service. Although the

multi-layer model has applicability to any organization which intends to use it for its internal or external communication or information sharing, Flexible to implemented in phases , Simplicity to make sense to a non security or IT expert. And it can be used as a tool to assess the level of security readiness of government departments, used a checklist for the required security measures, and as a common reference for the security in the government departments (Alazazi, s., 2008), but it lacks the existence of mathematical methods for assessment, would provide a set of integrated security readiness indicators and establish security requirements easily that protect information sharing between the e-government organizations from various risk sources. It lacks the existence of an application model that eases its practical use. In addition, the limited validation process was conducted in Dubai only.

The work of this thesis is concerned with the development of this target model, and with selecting case-study in order to investigate practical, test the validity and increase its usability. On the other hand, The Yemeni government trying to find the appropriate e-government framework to enhance the economical growth and provide the people with the best and fastest services offered by new technology, by examining the e-government literature, it was found that there was a lack of research that can assist in evaluating the e-government situation in the Republic of Yemen (Alsohybe, 2007).And according to (Alsohybe, 2007) the

challenges facing the Government of Yemen is the trust of the Yemeni citizens and organizations to exchange information. In Yemen the results revealed that 85% of the participants think that security will be a major problem along the road of e-government implementation. Most participants do not trust online transaction and transfer of important personal and organizational information.

Therefore, this thesis is concerned with the development of the target model, and provides a new mathematical model with selecting Yemen e-government a case-study in order to investigate practical to test the validity of the new model.

1.4 Research Questions

This study attempted to answer the following questions:

1. What are the assessment security readiness indicators for implementing of e-government in Yemen organizations?
2. What are the security challenges that influence the Implementation of e-government initiatives in the government of Yemen?
3. What are the security requirements to develop of Information Security Readiness Indicators for the Implementation of E-government in Yemen?

1.5 Research Objectives

The main objectives of the research were as follow:

1. Developing of a mathematical model that provides a new approach for assessment; this approach introduces an analytical method for assessment, which accommodates the various factors considered, both individually and collectively, according to the multilayer model layers.
2. Using of the model for the investigation of information security readiness in Yemen government organizations for implementation of e-government. This object has the following sub-objects :
    a) Assessing of security readiness for the implementation of e-government in the Yemen's organizations.
    b) Identifying the current status of information security and clarifying strengths and weaknesses points, for Yemen's government organizations.
    c) Identifying the security challenges that influence the Implementation of e-government initiatives in the government of Yemen.
    d) Establishing the security requirements for Yemeni's organizations to implement of the e-government.
    e) To provide a security model for Yemen e-government.
    f) To provide recommendations that can assist the government of Yemen in the implementation of the e-government.

1.6 Research Contribution

The work has the following contributions for researchers and government

- It provides a new approach for assessment of security readiness indicators, based on a mathematical model according to the multi-layer model.
- This research will help decision makers and employees on the implementation of e-government in Yemen to overcome some of the problems and challenges that await them in the future during implementation.
- This research is a useful source and literature review for the e-government security.
- Finally, The importance of the research, it's first study in this field in Yemen.

1.7 Research Methodology

This research applies research methodology mixing the quantitative and qualitative methods. The case study approach was used, is considered both qualitative and quantitative approach. The illustrative case study is useful in two main ways. They show security readiness status of the Yemen E-government and illustrating their specific strengths

and weaknesses points that would help them in the future security plans. They also show how the developed multilayer model analytical approach can be applied to practical investigations. The use of questionnaires was main source of the data analyzed, an analysis and a review of other available data, related documents on e-government projects, documents related with e-government security, models, and researches mentioned.

1.8 Limitation of the Study

This study is limited to the government sectors in Yemen's government. In addition, this study evaluates the security readiness within this sector in Yemen only, to exchange or share information between organizations.

1.9 Organization of the Thesis

This research is divided into six chapters.

Chapter One focuses on the introduction of the research as well as background of the research, research problem, research objectives, research questions, significance of the research and related terms and definition of this research.

Chapter Two includes literature review related to e-government security, security models, and multi-layer model components and give a view about Yemen's e-government.

Chapter Three covering the research methodological approaches used in the study, which in this case was mixed methodology. It contains detail description of qualitative and quantitative research designs, sampling plans, data collection instruments, data collection measurements, and data analyzing methods, validity and reliability.

Chapter four introduces the mathematical model for multi-layer model for assessment e-government security and describes the method of assessment the security readiness indicators at all layer.

Chapter five includes analysis of findings using support graphs, tables, other ways of presenting, and clarifying results.

In final, Chapter six includes detailed information about the study, findings & discussion of the findings, and how they relate to the e-government security. It relates the findings to the research objectives, discusses limitations of the study and offer recommendations for future.

1.10 Glossary of Terms

(Tayeh, 2008)

- **E-government (EGOV)**

E-government (EGOV) is defined as the delivery of services and information, electronically, to businesses and residents, 24 hours a day, seven days a week. E- Government is not limited to Web-based services(Norris, Fletcher, & Holden, 2001), (Liu, 2001).

- **Government**

Government is the means by which society pursues essential objectives: maintaining collective security, administering justice, providing the institutional infrastructure of the economy, ensuring that vital social capital is enhanced through improvements in health and education and through strong families and communities(Dawes, Bloniarz, & Kelly, 1999), (Liu, 2001).

- **Information System (IS)**

Information System (IS) refers to a physical process that supports an organizational system by providing information to achieve organizational goals(Turban, McLean, & Wetherbe, 1996), (Liu, 2001).

- **Information Technology (IT)**

Information Technology (IT) refers to the technological side of an information system, including hardware, databases, software networks, and other devices and can viewed as a subsystem of an information system(Turban, McLean, & Wetherbe, 1996), (Liu, 2001).

- **Threat**

A threat is simply any event that, if realized, can cause damage to a system, and create a loss of confidentiality, availability, or integrity (Coelho, 2007).

- **Virus**

A computer virus is a malicious program designed to damage network equipment, including stand-alone computers (Coelho, 2007).

- **Worms**

Worms are programs that reproduce by copying themselves through computers on networks (Coelho, 2007).

- **Certification**

is the procedure by which a third party gives written assurance that a product, process or service conforms to specified requirements (Manuel, 2006).

- **DDos (Distributed denial-of-service)**

just a virulent strain of denial-of-service attacks, meaning there is no single source of the attack. Denial-of-service does harm just by the attempt to deliver packets; whether or not the packets would authenticate properly is completely irrelevant. They stop something from working, such as attacks and session hijacking. Denial-of service attacks work because computer networks are there to communicate (Manuel, 2006).

- **Information Communication Technology**

Technology that deals with the storage, processing and dissemination of information especially using computers (Manuel, 2006).

- **Information**

An asset, like other important business assets, has value to an organization and consequently need to be suitably protected (Manuel, 2006).

- **Information security**

the protection of information and the systems and hardware that use , store and transmit that information to ensure business continuity, minimize business damage and maximize return on investments and business opportunities (Manuel, 2006).

- **ISMS**

Information Security Management Systems is the means by which Senior Management monitor can control their security, minimising the residual business risk and ensuring that security continues to fulfil corporate, customer and legal requirements (Manuel, 2006).

- **Fraud**

Deliberate deception or cheating intended to gain an advantage. Fraud has been attempted against every commerce system ever invented, neither will the criminals' techniques (Manuel, 2006).

- **Standard**

A technical or procedural specification, or both, that is significant and should be followed(Manuel, 2006).

- **Asset**

Anything that has value to an organization(Coelho, 2007).

- **Confidentiality**

Ensuring that information is accessible only to those authorised to have access (Coelho, 2007).

- **Risk assessment**

The overall process of risk analysis (systematic use of information to identify sources and to estimate the risk) and risk evaluation (process of comparing the estimated risk against given risk criteria to determine the significance of risk (Coelho, 2007).

- **Risk management**

Coordinated activities to direct and control an organization with regard to risk (Coelho, 2007).

- **Risk treatment**

Process of selection and implementation of controls to modify risk .]. In practical terms, treat the risk can be (1) reduced by security controls; (2) transferred its negative effects to another party through e.g. insurance; (3) avoid the risk by preventing the use of the asset affected by that risk (Coelho, 2007).

- **Security control**

A practice, procedure or mechanism that mitigates security risk . A list of recommended security controls. Examples studied in this research are ISO(Humphreys02b).

- **Vulnerability**

A weakness of an asset, a flaw in the organizational policies or worker's actions, that allows a threat to cause harm(Coelho, 2007).

1.11 Abbreviations

CIO	Chief Information Officer
CIW	Certified Internet Webmaster
CISSP	Certified Information System Security Professional
DDoS	Distributed Denial of Service
DoS	Denial o Service
E-GOV	Electric government
ICT	Information and Communication Technology
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System

IPsec	Internet Protocol Security
IS	Information Systems
IT	Information Technology
ITU	International Telecommunication Union
G2B	Government-to-Business
G2C	Government-to-Citizen
G2E	Government-to-Employs
G2G	Government-to- Government
MIS	Management Information System
NIST	National Institute of Standards and Technology
S-readiness	Security readiness
SANS	System Admin. Audit Network Security
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
VPN	Virtual Private Network

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter contains four parts; the first part describes concepts of the e-government and Yemen e-government background. The second part covers concept of the e-government security, policy, and threats. The third part covers the literature review of the security models. The final part covers multi-layer model component.

2.2 E-government Background

A number of definitions for e-Government have been given in existing literature. Many terms such as “digital government”, inter-networked government” (Tapscott, 1995) and” government online” has been used. The researcher deems all these terms to be synonymous. The (OECD, 2003) defines e-government as “the use of information and communication technologies, and particularly the internet, as a tool to achieve better government”. In this description, the internet is defined as

a requirement and a possible medium for e-government. It also emphasises that ICT and the internet should be viewed as tools for better government, not as goals to be achieved in their own right. E-Government in simplest terms can be described as the use of ICT within government to make operations more efficient, improve quality of service and offer an easy access for citizens to government information and services (Kraemer and King, 2003).

From these definitions it can be concluded that e-government is a system that literally engages and covers every entity in its area of authority (i.e. citizens, businesses and public organizations).

2.2.1 E-government Applications

E-government offers services to those within its jurisdiction to transact electronically with the government. These services differ according to users needs and ICT capacity, and this diversity has given rise to the development of different applications of e-government, described in the following subsections:

2.2.1.1 Government to government (G2G)

This category of service includes improving the efficiency of

transaction and business functions within itself or with other governments (David and Evans, 2005). In order to recognize the importance of single access point, association and cooperation along with different governmental departments and agencies is required. Valentine (2004) said that G2G build relationship with organizations, such as national, local, regional and with other foreign government organization. It allows the government to eliminate unemployment, crime, and homeland security. For this act government has introduced intergovernmental assistance, amplify the emergency helpline response, and connection of law enforcement agencies. The G2G provide cooperation of both external and internal agencies and improve service inside or outside of governments (Fang, 2002).

2.2.1.2 Government to Business (G2B)

In G2B government can acquire items, pay invoices, and perform other business activities in a more beneficial way. Obtaining data to scrutinize and assist in decision making can be done, to support the government through G2B. David and Evans (2005) mentioned that, this category focuses on the ability to cut the cost, collect information and make better

inventory control. Some of the advantages for this type are the online regulations availability for agencies and increasing electronic tax facilities for industry. It also creates an electronic market place for government and reduces red tape, makes the process more easy and help in establishing a web presence fast and cheaper (Valentine, 2004).

2.2.1.3 Government to Citizen (G2C)

According to (David and Evans, 2005), this group of service keeps an eye on the activity of government and citizen to exchange information to each other in a competent and electronic way. (Valentine, 2004) identified that G2C allows citizen to access electronic government services anytime, directly and conveniently through the use of various channels (PC, WebTV mobile phone or wireless device). The citizen can get benefits from this government information. A primarily benefit of G2C is the simple posting of forms and applications online, 24/7 services are available through the Internet.

2.2.1.4 Government to Employees (G2E)

This group of service consist of relationship between government and its employees (Fang ,2002). Valentine (2004) He further explained

that it gives the possibilities to employees to accessing the policies related to compensation and benefits. G2E another large area which requires a full attention G2E facilitates the management and communicates with government employees in order to make e-career and e-office.

2.3 E-government initiative project in Yemen

The Yemen government, like most other developing countries, is still trying to implement IT in government organization, and try establishing some projects as initial step to make e-government such as the National Program for Information Technology, that known as Yemen e-government project (MCIT, 2003).Table 2-1 compare Yemen to other countries around the world and show that Yemen is still one of the lowest countries in term of E-government development between “2008-2010”.

Table 2-1: E-government development for Some Countries Including the Yemen between (2008-2010)

Country	E-government development index value		World e-government development ranking	
	2010	2008	2010	2008
Bahrain	0.7363	0.5723	13	42
Cyprus	0.5705	0.6019	42	35
United Arab Emirates	0.5349	0.6301	49	32
Kuwait	0.5290	0.5202	50	57
Jordan	0.5278	0.5480	51	50
Saudi Arabia	0.5142	0.4935	58	70
Qatar	0.4928	0.5314	62	53
Turkey	0.4780	0.4834	69	76
Oman	0.4576	0.4691	82	84
Azerbaijan	0.4571	0.4609	83	89
Lebanon	0.4388	0.4840	93	74
Georgia	0.4248	0.4598	100	90
Armenia	0.4025	0.4182	110	103
Syrian Arab Republic	0.3103	0.3614	133	119
Iraq	0.2996	0.2690	136	151
Yemen	0.2154	0.2142	164	164

Source : United Nations E-Government Survey 2010

According for ESCWA report(ESCWA,2009) ,Since the announcing of the e-government initiative and the opening of its website in 2003, the initiative came to a stand - still, due to lack of readiness of an environment conducive to this transformation. Most of the agencies and institutions are still below the required standard. The majority of information systems available to the authorities lack the technical component compatibility, which reflects negatively on the possibility of networking with each other. Finally, a website for the

government was launched, through which it will be possible to publish information relating to the activities of various Government agencies. On the other hand, electronic services offered to citizens are still in their infancy; whereby no transactions or procedures can be fully processed electronically. Other than that, most government institutions provide information about the services they offer to the citizens who need them and steps needed to obtain any of the services they provide, in addition to providing the forms used to obtain a service. Some government institutions tried to provide additional forms for citizens to fill out and send in-order to get a specific service. With the exception of the Law issued under number 40 in the year 2006 concerning payment and electronic financial and banking transactions, there are no complete and applicable legislations in Yemen today in the field of security of electronic transactions and networks and ensuring their security. However, a draft of the information law to be discussed by Parliament according to the proposal of the National Information Center contains a separate section on information security. That, in addition to the initiative announced by the Ministry of the Interior concerning its endeavors to prepare a draft law to combat cyber crime, but this initiative is still in its early stages. the currently

used information security measures are at a low level, whereby the use of simple ways of protecting and securing data and information is the most common. This is due to informatics being a new science, and thus the legal regulation of this area is still in its infancy. The most important initiative in this area is the Yemeni government's intention to prepare a draft law to combat cyber crimes with the objective of controlling crimes associated with the scientific advance in the field of informatics. The National Information Center presented a "draft of information law that guarantees the right of access to information and greater transparency and protects privacy. It is being currently studied in the Legislative Council.

From the last and after review to document e-government project known as the National Program for Information Technology and other literature associated with this project (MCIT, 2003), the following has been noted on the e-government project : Lack of vision , policies , plans, legislation , laws , and lack of coordination between the ministries and institutions of national information project to ensure that they complement each other in various aspects and to reduce the effort and expense, including for example; Information System Civil Service Project, National network of information project, networking project

between the universities of Yemen, labor market information system Project, Information System project and financial accounting and Information system of the judiciary Project.

2.4 E-Government Security

Security in government is not a new concept. Since antiquity politicians, military leaders and other government "agents" have been trying to protect "sensitive" information from unauthorized or accidental loss, destruction, disclosure, modification, misuse or access (Tassabehji, 2005a). Information systems, which are the foundation of e-government, are recognized as socio-technical infrastructures that rely heavily on people. This is particularly true in the case of security, where human factors have played a major part in many security failures (Weirich and Sasse 2002). As such, best practice of security management takes a holistic organizational approach which incorporates an organization's business processes, controls and policies; corporate governance; human resource management and training; and organizational culture as well as systems and technology infrastructures. (Higgins 1999; Gelbsein 2001; Tassabehji 2003; Tassabehji 2005b). Along with security are issues of privacy of

information and trust of users or citizens which is a superset of security (Patton & Josang 2004) also identified in e-commerce literature as a main obstacle in the growth and adoption of e-commerce (Tassabehji, 2003, Yousafzai et al 2005). However, for e- government, issues of security are even more critical as the government is held to a higher standard of security than commercial organisations because of the sheer magnitude of its operations, the additional socio-politico-ethical dimensions of the universality of its service delivery to all its citizenry, and its consequent attractiveness as a target for hackers (Plexico, 2000).

2.4.1 E-Government service attacks and threats

Security threats are "circumstances that have the potential to cause loss or harm" to information security (Pfleeger, 1997).The following are the e-government service attacks and threats (Cabinet Office , 2002):

- **Unknown Outsider Attack:**A hostile outsider may gain direct access to e- Government services with the objective of achieving some personal gain or causing damage to the system.
- **User Fraud:** A legitimate user or other client of e- Government services may submit a false transaction or deny obligations in respect of transactions submitted.

- **Insider Attack:** An individual with privileged access to government data networks may abuse that position to create false transactions or interfere with legitimate transactions.
- **Privileged Insider Attack:** An individual with privileged access to, or management responsibility for, e-Government service provision may abuse that position to interfere with or exploit service provision.
- **False Identity:** An individual may establish false or multiple real-world identities to access e-Government services and submit fraudulent claims or cause other damage to the service.
- **Impersonation:** An individual may impersonate a legitimate client or other user or operator in order to secure services on that user's behalf.
- **Unauthorized Disclosure:** Personal information or other information submitted as part of an e-Government transaction may be disclosed to those with no need or rights to access it.
- **Revoked Rights:** Those who have in the past possessed rights of access to e-Government resources may misuse those rights after they have, or should have been, revoked.
- **Theft of Access Tokens:** Access tokens that confer rights with

respect to e-Government services may be stolen and used for improper purposes.

- **Duplication of Access Tokens:** Access tokens that confer rights with respect to e-Government services may be duplicated and copies used for improper purposes.
- **Capture of Access Credentials:** Access credentials may be captured and used for improper purposes.
- **Denial of Service Attacks:** Threat agents may seek to deny access to the e-Government services by legitimate users.
- **Misinformation and Propaganda:** e-Government services, and hence use of the service, may be undermined by laying a trail of false and misinformation which purports to carry the authority of government by virtue of its apparent association with the e-Government service.
- **Breach of Anonymity**: Transactions that are required to be anonymous may be traced to their originator and the association misused.
- **Breach of Accountability:** Clients or other users of e-Government services, and the departments offering the services, may not be able to be held accountable for attempted fraud or

maladministration.

- **Failure to Recover Business Information:** Information assets contained within the system may become inaccessible if the access credentials are lost or unobtainable.
- **Loss or Theft of Monetary Value**: Monetary value owned by e-Government systems may be improperly disbursed.
- **Challenge to System Veracity**: It is possible that a user may disavow a transaction with a claim that the e- Government system was imperfect.

2.4.2 Information Security Policy

- An information security policy is a plan identifying the organizations vital assets with a detailed explanation of what is acceptable, unacceptable and reasonable behavior from the employee in order to effectively ensure information security (Hone & Eloff, 2002). For Nijhof (2003) policy is "an instrument for responsibilisation within the organization". An information security policy is a combination of principals, regulations, methodologies, techniques and tools (Tryfonas, 2001) established to protect the organization from possible threats. These policies

will help an organization to define their information assets and define its attitude to information (Canavan, 2003).David (2002) states that "Security is not what you do, it is not what you do not do, it is not what you allow, and it is not what you prevent. Security has nothing to do with how safe your data and system Security is how well you adhere to your formal security policies". The purpose of the security policy is "to create a shared vision and an understanding of how various controls will be used such that the data and information is protected in an organization" (Dhillon, 2006). Zuccato (2004) states that security policies are used to obtain security requirements for organizations, in terms of what they want to protect and how to protect it.

2.4.3 Criteria of an Effective Information Security Policy

There are some criteria that the information security policy needs to consider to give good results in securing organizational assets. These criteria have been summarized by different authors Baskerville & Siponen (2002); Madigan (2004); and Luker & Petersen (2003). According to (Awadi, 2009) the policy must:

- **Fit the organizational culture:** the security policy of an

organization mostly depends on the common organizational culture. Organizations differ in their security requirements. What is suitable to one organization may not be suitable to another.

- **Have a style which is consistent with the organization's general communication style:** a common format makes the policy easier for employees to understand the purpose of it.
- **Be effective and dynamic:** organizational policy should be revised and changed regularly, a minimum period of time could be six months or less to avoid any threats from happening and help to also define new threats;
- **Easy language:** Not described as a technical document, but uses simple language to ensure it is not difficult to understand. It should be free of jargon or technical terms, easy to understand and also be written in a solid language rather than an abstract language to stop any confusion for employees regarding policy.
- **Specify the job responsibilities:** allow employees to find out what their responsibilities are and what they are required to do to follow the policy;
- **State the purpose of the policy and the scope of the organization:** the policy has to state the reasons for the policy

and what the organization's aim is, in order to let the employees understand the benefit of such policy; and

- **Explain what activity is acceptable and what is not:** this will make it clear to employees what is acceptable behavior and what is not.

2.5 Information Security Models and standards

Security models are fundamentally important security design and analysis tools. A security model provides a template for security policy enforcement in a system. While most security models cover the same topics, the approaches may vary (Liska .A.,2003).On other hand, the Security standards address the minimum mandatory rules an organisation is required to follow in order to provide an acceptable security level (Karabacak, B. and Sogukpinar, I., 2005). Having a security model that addresses technology only and implemented across multiple organisations will be a challenge unless the model is complemented by security standards and policies Models alone will not provide comprehensive security programme to the organisation. In this section, well known general security models types and security standards will be addressed to reflect the applicability in different types

of organizations.

2.5.1 Bell-LaPadula model

The Bell-LaPadula model was the first mathematically specified information flow security model. It has been formally proven that, if its conditions (four security levels and three main rules) are properly implemented, then information can only flow in a secure way between subjects. The model is considered as a multilevel security model. The model was implemented in many systems which became known as multilevel secure systems (Anderson, R., 2001).

2.5.2 Chinese Wall model

The Chinese Wall model was developed by Brewer and Nash (Brewer and Nash, 1989) to prevent any conflict of interest with an organization or between an organization and its clients. This model is able to represent a security policy that deals equally with confidentiality and integrity, and is hence useful for the business environment. Indeed, it even complies partly with British law, which requires use of policies similar to that instantiated by the Chinese Wall model (Bishop. M. ,2005). The aim of this model is to ensure that the data of two different

users stay separated, regardless of the levels of sensitivity of the data themselves.

2.5.3 Non-Interference model

The non-interference model was developed by Goguen and Mesguer in 1982 (Goguen, J. A. and Mesequer, J., 1982).The noninterference property can be used to ensure that any actions taking place at a higher security level do not interfere with those taking place at a lower security level. This ensures that users at a lower security level cannot discover which commands are being executed by users at a higher security level.

2.5.4 Biba model

The Biba model addresses data integrity, using an information flow approach. The integrity property is represented as a set of ordered integrity levels; the higher the level, the more confidence users can have that (Bishop. M., 2005).The Biba model or as known "Bell-Lapadula upside down" was developed by Ken Biba. The model addresses the integrity aspects only and does not address the other two aspects of C.I.A (confidentiality, Integrity, Availability) triad. Neither

the Bell-LaPadula nor the Biba model provide a way to define security and integrity ratings, and to make modifications to such ratings; they also do not deal with delegating or transferring access rights (Harris. S., 2003).

2.5.5 Non-deducibility model

The Sutherland's non deducibility model developed in 1986. The model explicitly explains that information can flow from high-level objects to low-level objects if and only if some possible assignment of values to low-level objects in the state is inconsistent or conflicting with a possible assignment of values to the state's high level objects (McLean, J., 1990).

2.5.6 BS7799 standard

The British standard was originally launched in 1999 and was named as BS 7799-2:1999 and was changed to ISO/IEC 17799 in 2005 (Karabacak, B. and Sogukpinar, I., Sept 2006). British Standard 7799 covers the management of information security. The purpose of ISO/IEC 17799 is to assure the confidentiality, integrity and availability of information assets of the organisation by using a set of controls,

which could be good practice, policies, organisational structures, software functions or procedures. It is intended to provide a common basis for developing organisational security standards and effective security management practices that provide confidence in inter-organisational dealings (ISO 17799). The standard is divided into 10 sections, with 36 objectives. Each objective is again divided into sub-objectives. The 10 sections can be summarised as follows:

- **Security policy:** Aimed at providing management with the direction and support for information security
- **Organisational Security:** Consists of three sections. First is the information security infrastructure which aims at managing information security within the organisation. Secondly, security of third-party access, with the aim of maintaining the security of organisational information processing facilities and information assets accessed by third parties. Thirdly, outsourcing, aimed at maintaining the security of information when the responsibility for information processing has been outsourced to another organisation.
- **Asset classification and control:** Consisting of two sections. First, accountability of assets with the objective of maintaining

appropriate protection of organisational assets. Secondly, information classification with the goal of ensuring that information assets receive an appropriate level of protection.

- **Personnel security:** Aimed at reducing the risks of human error, theft, fraud or misuse of facilities. Secondly, to ensure that users are aware of information security threats and concerns, and are equipped to support organisational security policy in the course of their normal work. Finally, to minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.
- **Physical and environmental security:** To prevent unauthorised access, damage and interference with business premises and information. In addition, to prevent loss, damage or compromise of assets and interruption to business activities.
- **Communications and operations management:** To ensure the correct and secure operation of information processing facilities, and maintain the integrity and availability of information processing and communication services.
- **Access control:** To control access to information.
- **System development and maintenance:** To ensure that security is

built into information systems.

- **Business continuity management:** Aimed at offsetting interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.
- **Compliance:** To avoid breaches of any criminal and civil law, whether statutory, regulatory or contractual. Secondly, to ensure compliance of systems with organisational security policies and standards, taking system audits into consideration.

2.5.7 BSI IT baseline protection manual

This standard was developed by German Bundesamt Fur Sicherheit. The standard covers controls to safeguard organisations. The main goal of the standard is to achieve a security level for IT systems that is reasonable and adequate to satisfy normal protection requirements and can also serve as the basis for IT systems and application requiring a high degree of protection.

2.5.8 COBIT

Control Objectives for Information and related Technology (COBIT) is another approach which has been developed by the IT

Governance Institute of Information Systems Audit and Control Association (ISACA). COBIT is a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IT audit, control and security practitioners (ISACA, 2005). COBIT defines control as "the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected" (ISACA, 2005). COBIT positions itself as the tool for information technology management and refers, amongst many issues, to information security.

The last version of COBIT 4.0 was released in 2005 and it has 34 high-level control objectives or processes are referred to in some journals grouped in 4 domains (Hardy, G. (2006) :

- **Plan and organise:** This domain covers strategy and tactics, and concerns the identification of the way ICT can best contribute to the achievement of the business objectives. Furthermore, the realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. This includes proper organization as well as the technological infrastructure that must be

in place.

- **Acquire and Implement:** To realise the ICT strategy. ICT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the life cycle is continued for these systems.
- **Deliver and Support:** This domain is concerned with the actual delivery of required services, which ranges from traditional operations over security and continuity aspects to training. To deliver services, the necessary support processes must be set up. This domain includes the actual processing of data by application systems, often classified under application controls.
- **Monitor and Evaluate:** All ICT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management's oversight of the organization's control process and independent assurance provided by internal and external audit or obtained from an alternative source.

COBIT was found as a good model to use not exclusively for

information security.

2.5.9 The Multi–layer model

The Multi –layer model was developed by Alazazi in 2008(Alazazi, s., 2008).The model has five layers; each layer is important and assists the organization to achieve a milestone within the security field. The top layer of the model represents the most common in the security field. Security technologies are always implemented and with the proliferation of the Internet access, they became integrated as part of the business support systems. The second layer, the security policies, complements the first one. Security practitioners develop security policies for their organizations and attempt to place technologies in order to tighten the security policies and prevent them from becoming self- defeated policies. The third layer, the security competencies, the security competencies are needed for the development of the technologies and security policies. The fourth layer, the security operational and management procedures, having the proper operational and management procedures are an art and will need to be monitored and evaluated periodically. The fifth layer, the security decisions, the management

decisions to launch an e-service or implement a security technology for the organization impact on all the previous layers. Figure 2-1 illustrates the Multi–layer model layers

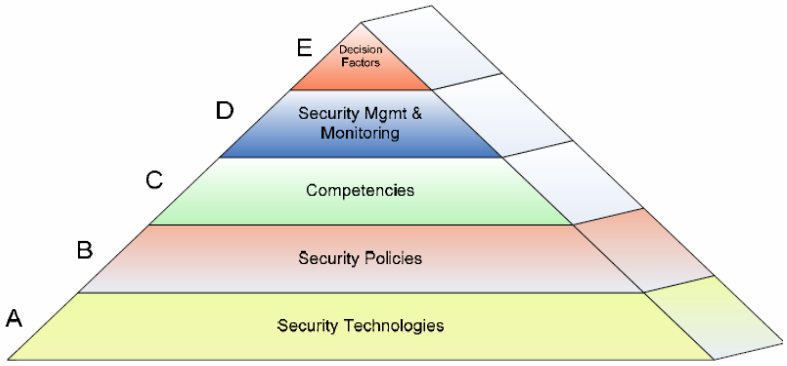

Figure 2-1: The Multi–layer model layers: (Alazazi, s., 2008).

2.6 Comparison between Security models and standard

This section illustrates the comparison between all models and standards according to the following characteristics (Alazazi, s., 2008):

- **Structured in layers:** The models are divided to same layers.
- **Coverage of security aspects:** The main areas of security (technology, policy, operation, human aspects, etc) addressed by the model.
- **Explicitly explained:** The literature explained the models in detail.

- **Government or commercially used:** The models are used by government and non government organizations.
- **Applicability to any sector:** The model can be applied to any sector or industry.
- **A dressing information flow:** The model addressed information flow within a system or addresses the flow of information across multiple systems/networks.

Table 2-2 summarizes the information security models and compares them.

Table 2-2: Comparison between Security models and standards :(Alazazi, s., 2008).

Characteristics	Models and Standards								
	Non Deducibility	Non Interference	Bell Lapaduka	Biba	Chinese wall	BS7799	BSI IT	COBIT	multi-layer
Structured in Layers	x	x	x	x	x	x	x	x	√
Coverage of Sec Aspects									
Technology	x	x	x	x	x	x	x	x	√
Policy	√	√	√	√	√	√	√	√	
Human behavior and awareness	x	x	x	x	x	x	x	x	√
Ops and Mgmt	x	x	x	x	x	√	√	√	√
Explicitly explained	√	√	√	√	√	√	√	√	√
Government or commercially	√	√	√	√	√	√	√	√	√
Applicability to any sector	√	√	√	√	√	√	√	√	√

Address Info flow									
Within One System or entity	√	√	√	√	√	x	x	x	√
Within Several Systems	x	x	x	x	x	√	√	√	√

The majority of the models above are not addressing more than one aspect of information security and focus on the security of a single system or node. It has also been observed that the above models are not structured in terms of layers and modeling principles. And The security standards illustrated above are cover the majority of all security aspects. The only gap that they have is their missing of the competency aspects of the security team and the cost of the implementation of the standards. The different standards which make it difficult for the management of the organizations to understand and grasp which one to use. Table 2-2 illustrated above the Multi–layer model cover all security aspects, models and standards such as the competency aspect which was not addressed by the other models researched, the decision aspect which was missed out from most of the security models in the field of information security and the link between all the five layers which gives any security model a strength to stand as an independent security program.

Due to these reasons, we will adopt the multi-layer model for further development and investigate its use to asset the information security of e-government in Yemen.

2.7 The Multi-layer Model Components

This study illustrates the multi-layer model component and summarizes it as follows:

2.7.1 The security technologies layer

This layer consists of number of the security technologies that has been shown in Table 2-3, these technologies are as follows:

Table 2-3: Technology layer :(Alazazi, s., 2008)

Factor
Access Control
Intrusion Detection and Prevention
Anti-Virus & Malicious Code
Authentication and Passwords
Files Integrity Checks
Cryptography
VPN
Vulnerability Scanning Tools
Digital Signatures and Certificates
Biometrics
Logical Access Control (Firewalls)
Security Protocols

2.7. 1. 1 Access Control

Access control is the process of granting or denying specific requests to obtain and use information and related information processing services; and enter specific physical facilities (NIST, 2010). Access control used to ensure that only authorized individuals are allowed to add, view, modify, or delete specific resources. Access controls are the fundamental building blocks for all other security services. Authentication and authorization are two major functions in providing access control services.

2.7. 1.2 Intrusion detection and prevention

Intrusion detection systems (IDS) Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents(NIST ,2010). Intrusion Detection: Intrusion detection and prevention systems (IDS & IPS) monitor either network traffic and/or host's behaviour and can either generate alerts or take direct action in the event that suspicious network traffic or host behaviour is detected. IDS product typically generate alerts, while IPS products can terminate active TCP connections, and

even disable services, systems, or even entire subnets in response to detected attacks of malicious activity.

2.7. 1.3 Anti-virus & malicious codes scanners

Anti-virus is A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents (NIST, 2010). Due to the need of exchanging files and information between the e-government departments, the lack of having a proper antivirus solution with a full synchronization of viruses updates, the probability of having an e-government department getting infected with viruses from another department due to unsecure file exchange over the Internet is high (Alazazi, s., 2008).

2.7. 1.4 Authentication and passwords

Authentication is The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. A process that establishes the origin of information or determines an entity's identity Verifying the identity of a user, process, or device, often as a prerequisite to allowing

access to resources in an information system (NIST ,2010).Passwords is a protected character string used to authenticate the identity of a computer system user or to authorize access to system resources ,its a secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings (NIST, 2010).

2.7.1.5 Files integrity checks

Files integrity checks are Software that generates, stores, and compares message digests for files to detect changes to the files (NIST ,2010).Integrity check is not commonly used and sometimes is overlooked by security practitioners due to the lack of good tools and mechanism in the organisation. Different tools can be used to ensure the data integrity such as digital signatures, certificates or hashing mechanism (Jaeger, T. and Rubin, A. D., 1996).

2.7. 1.6 Cryptography

According to (NIST, 2010) Cryptography is the discipline that embodies principles, means, and methods for providing information security, including confidentiality, data integrity, non-repudiation, and authenticity. It is categorized as either secret key or public key. Secret

key cryptography is based on the use of a single cryptographic key shared between two parties. The same key is used to encrypt and decrypt data. This key is kept secret by the two parties. Public key cryptography is a form of cryptography which makes use of two keys, a public key and a private key. The two keys are related but have the property that, given the public key, it is computationally infeasible to derive the private key. In a public key cryptosystem, each party has its own public/private key pair. The public key can be known by anyone; the private key is kept secret.

2.7. 1.7 Virtual private network (VPN)

A virtual network, built on top of existing physical networks, that provides a secure communications tunnel for data and other information transmitted between networks (NIST, 2010).Virtual Private Networks (VPN) Provide encrypted access via the Internet or other non - trusted networks to e- Government system, and allow for authentication, which ensures that only individuals who have been authorized to access the systems are able to do so.

2.7. 1.8 Vulnerability scanning tools

Are tools that scan the weakness in an information system, system

security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. E- Governments need scanners and tools for scanning the internal and the external vulnerabilities.

2.7. 1.9 Digital signature and digital certificates

Digital signature is An asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection (NIST, 2010).according to Alazizi(2008),e-governments used it for authorization, authorization, verification of customers information. Digital Certificates on the other hand are mechanisms and are issued by trusted third parties known as Certificate Authorities (CAs) (Tiwana, A.,1999).

2.7. 1.10 Biometrics

Biometrics is a physical or behavioral characteristic of a human being. It's a measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics (NIST, 2010). Biometrics are used in payment

systems to prevent fraudulent claims (Tipton, H. F. and Krause, M., 2000).

2.7. 1.11 Logical access control (Firewalls)

Firewall is a hardware or software capability that limits access between networks and/or systems in accordance with a specific security policy(NIST, 2010). It is used a gateway to allow or block traffic between networks in accordance with security policy . It used to filter inbound and outbound traffic to and from systems in the e-Government network, and between different network enclaves within the Government networks.

2.7. 1.12 Security protocols

Security Protocols such as IP Security (IPsec) and Secure Socket Layer (SSL) act as a proactive mechanism in providing security to information. IP Security (IPsec) is Suite of protocols for securing Internet Protocol (IP) communications at the network layer, layer 3 of the OSI model by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for cryptographic key establishment(NIST, 2010).Secure Socket Layer (SSL) protocol used for

protecting private information during transmission via the Internet(NIST, 2010).Security protocols can be categorizes as either network layer or application layer ones (Huth, M. R. A., 2001).

2.8 Security policies layer

This layer consist of number of security policies such as password management, log-in process, logs handling, computer viruses, intellectual property rights, data privacy, privilege control, data confidentiality, data integrity, Internet connectivity, administrative policies, encryption policies, HR security policies, third party policies, physical security policies, and operation security policies. Table 2-4 show the policies for the model.

Table 2-4: Policy layer :(Alazazi, s., 2008)

Factor
Password Management
Log-in Process
Logs Handling
Computer Viruses
Intellectual Property Rights
Data Privacy
Privilege Control
Data Confidentiality
Data Integrity
Internet Connectivity

Administrative Policies
Encryption Policies
HR Security Policies
Third Party Policies
Physical Security Policies
Operation Security Policies

2.9 Security competencies layer

In this layer the researcher recommends number of competencies for the security practitioners, which will assist the government organizations enhancing the control of security and narrow the gap of the knowledge between the different government security organizations. It will contribute in elevating the trust on the security programmes between the government rganizations and will increase the usability of the e-services by the citizens due to the strong confidence in the security level of the government organizations. The knowledge of how to protect the e-government services will be the sole responsibility of the security practitioners involved directly with the e-government security department as direct employees or suppliers, consultants, or third parties to the e-government. The e- government authority must allow their security staff to get the maximum knowledge on various security areas such as hacking, computer forensics, etc. These competencies are recommended that the e-government authorities allow their security staff

to get updated on the security knowledge. There competencies are security operation and management, security architecture and development, ethical hacking, security policies development, computer forensics, cryptography, security programming, law and regulations, security implementation and configuration, and security analysis. Table 2-5 show the competencies for the model.

Table 2-5: Competency layer :(Alazazi, s., 2008)

Factor
Security Operation and management
Security Architecture and development
Ethical Hacking
Security policies and development
Computer Forensics
Cryptography
Security Programming
Laws and regulations
Security implementation and configuration
Security Analysis

2.10 Security operations and management layer

This layer consist of number of tools and functions which will ease the process and will allow the operational staff to contribute better in the analysis , response to attacks and needed to accomplish the security monitoring and management. The author believes that having this layer complements the other layers in the security model and makes them

more tied in the inter-functional requirements and processes. The sub layers indicated in Table 2-6 are the proposed tools and functions such as operational policies and procedures, management tools, correlation engine, data warehouse and data mining, reporting and response and analysis and human intervention.

Table 2-6: Operations and management layer :(Alazazi, s., 2008)

Factor
Operational Policies and procedures
Management Tools
Correlation and data mining
Reporting and Response
Analysis and human intervention

2.11 Security Decision layer

This layer consist of number of factors listed in Table 2-7, these factors play major role on whether a security programme can be successful or not. Each factor has a direct or indirect effect the other sub factors in the same layer as well as the other sub factors in other layers of the model. The cost of security technologies is a good illustrative point to the impact of the decision layer on other layers of the security programme. Considering the cost constraints of any organisation, having the best technology, right competency, end-to-end operation and

management infrastructure, and the right security policies will be evaluated thoroughly. Having the combination of all or some is also related to the cost limitation which derives the decision of the management of the organization. Awareness is another factor which derives the decision. Having the right awareness on technologies to select, policies to apply, required competencies, and the right level of management and monitoring will have an impact on which direction the organization can take.

Table 2-7: Decision layer :(Alazazi, s., 2008)

Factor
Cost
Awareness
Need
Technologies Availability

2.12 Chapter summary

This chapter contains four parts; the first part describes the concept the e-government and Yemen e-government background. The second part covers the concept the e-government security, policy and threats. The third part covers the literature review of the security models. The final part covers the multi-layer model component.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter describes the research methodology used for achieving the research goals. It describes strategy of the research design to the developing mathematical model and investigations by using case study that is Yemen e-government; analyzing the security readiness for implementation to e-government in Yemen. This chapter will also highlight the research population and sample design, Response rate and respondents representation, review of data collection tool which is the questionnaire survey and questionnaire validity.

3.2 Research process and Design

This study needs conceptual framework of the research design to follow up the expected results. Therefore, the best way to do this research is by having a design or a framework which can help to answer the research questions and directs the progress of the research by employing the

conceptual framework. Figure 3-1 shows conceptual framework for research design. This framework provides the design of the study and the research process to the developing mathematical model and investigation that can be by use of case study that is Yemen, assessment of security readiness for implementation in the e-government in the Yemen's organizations and identify the security challenges.

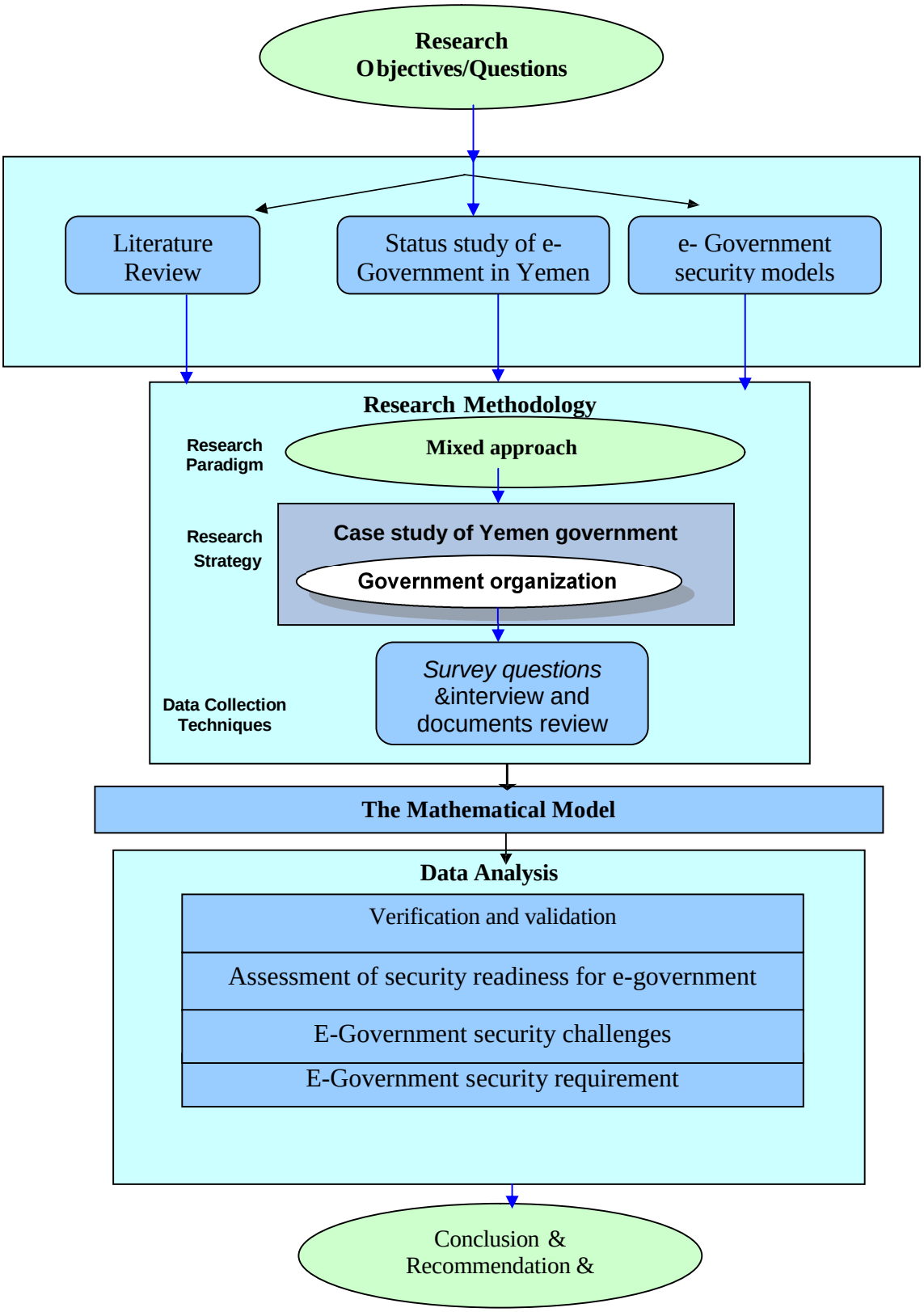

Figure 3-1: Research Design: the overall plan for conducting this research.

3.3 Research Approaches

To achieve the objective of the research study, as explained above, there are three different broad methodological approaches. According to (Swanson & Holton, 2005 & Creswell, 2003):

- Qualitative approach.
- Quantitative approach.
- Mixed approach.

3.3.1 Qualitative Research approach

Qualitative research is multi method in focus, involving an interpretive, naturalistic approach to its subject matter. This means that qualitative researchers study things in their natural settings, attempting to make sense of, or interpret, phenomena in terms of the meaning people bring to them (Newman & Benz, 1998).Qualitative approach is one in which the inquirer often makes knowledge claims based primarily on constructivists perspectives (i.e., the multiple meaning of individual experiences, meaning socially and historically constructed, with an intent of developing a theory or pattern) or advocacy/participatory perspectives (i.e., political, issue-oriented, collaborative or change oriented) or both. It also uses strategies of inquiry such as narratives, phenomenology,

ethnography, grounded theory studies or case studies. The researcher collects open-ended, emerging data with the primary intent of developing themes from the data (Creswell, 2003). Bjorck (2001) uses a qualitative method to study information security consultants' experiences and insights relating to the implementation and certification of information security management systems (ISMS).

3.3.2 Quantitative Research approach

Leedy and Ormrod (2005), state that quantitative study falls under the broad heading descriptive quantitative research. This type of research involves either identifying the characteristics of an observed phenomenon or exploring possible correlations among two or more phenomena. In every case, descriptive research examines a situation as it is. It does not involve changing or modifying the situation under investigation, nor is it intended to determine cause-and effect relationship. According to Cooper and Schindler (2003) a descriptive study may be simple or complex; it may be done in many settings. Whatever the form, a descriptive study can be just as demanding of research skills as the casual study. Leedy and Ormrod (2005) state that descriptive research designs and approaches involve observation studies, correlational research,

development designs and survey research. All of these approaches yield quantitative information that can be summarized through statistical analyses. In the field of information security many researchers use quantitative methods as part of their research. For example, a recent study by Workman (2007) uses a quantitative method to investigate social engineering attacks in the form of questionnaire in a field study of a government-regulated entity that experienced serious security breaches in the past.

3.3.3 Mixed Research approach

As implied by the name, mixed methods research combines or mixes quantitative research and qualitative research in the same study or a series of studies (Swanson & Holton, 2005). As such, mixed methods research is the third major research approach or paradigm (Johnson, Onwuegbuzie, & Turner, 2007). For mixed methods research, the classifications include four types (Swanson & Holton, 2005). In the first type, complementary, researchers combine the results of one method with the results of the other method (Swanson & Holton 2005). In the second type, development, the results from one method help develop or inform the other method (Swanson & Holton, 2005). For the third type, initiation,

the researchers recast the results from one method to questions or results from the other method (Ms.Douglas, 2010). Lastly, in the fourth type, expansion, researchers use different methods to extend the breadth or range of inquiry (Swanson & Holton, 2005).

The recent historical context of mixed methods research evolved from researchers and methodologists who believed in both qualitative and

quantitative research methodologies for addressing their research questions (Johnson, 2007). As such, the mixed methods research results in a synthesis that uses ideas from qualitative and quantitative research (Johnson, 2007). In addition, the researchers applying the concept of multiple operationalism, or triangulation, argue that the validity of findings from two or more research methods (QUAL/QUAN) enhances the belief that the results are valid and not artifact results of the single research methodology used (Johnson, 2007).

In this research, the researcher used mixed methods; the qualitative approach can be used to build mathematical model and to determine the security requirements and identify the security challenges. Quantitative method here is needed to calculate security readiness indictors, investigation for model and gather more information and illustrate clearer validation to the research.

3.4 Research Strategy

Research strategy is a general plan of how to answer the research questions that have beset (Saunders, 2000). There are many strategies available to carry out research studies. Creswell (2003) define some strategies associated to research method, which are:

3.4.1 Quantitative Methods

- **Experimental Research:** The purpose of experimental research is to study cause and affect relationships.
- **Survey research:** contains cross-sectional and longitudinal studies using questionnaires or structured interviews for data collection.

3.4.1 Qualitative Methods

- **Ethnographic:** This strategy will seek to understand the whole cultural group through the nature of their social structures and behaviors over a long period of time.
- **Grounded theory:** This strategy is not determined but derived from a general, abstract theory of a process, action, or interaction grounded in the views of participants in a study.

- **Case studies:** This strategy explores in depth a program, an event, a process, or one or more individuals.
- **Phenomenological research:** This strategy identifies the real meaning of human experiences. Rich & Ginsburg (1999) clarifies that this approach is about understanding humans through the meanings inherent in their experience.
- **Narrative research:** This strategy interprets human motivation, perceptions and behavior from reported stories about their lives.

Case study research is the most common qualitative method used in Information Systems and Information Technology (IS/IT) according to (Orlikowski & Baroudi, 1991; Alavi & Carlson,1992). A Case study research is generally descriptive, explanatory or exploratory (Gable, 1994; Yin, 2003). It combines data collection methods such as interviews, questionnaires and observations (Robson, 2002; Cooper & Schindler,2003). A case study is a well-suited research strategy for capturing the knowledge of practitioners and deriving theoretical propositions from it (Benbasat and Zmud, 1999).

For the purpose and scope of this research and appropriate technique is the case study of e-government in Yemen, it is useful in two main ways. They show the security readiness status of the E-government

illustrating their specific strengths and weaknesses points which help their future security readiness, and development plans. They also show how the developed multilayer model analytical approach can be applied to practical investigations. For this research, in particular which employed the use of survey research or questionnaires to collect data. During the development of the new model, a case study was needed in order to test the validity of the model. The motivations of selecting Yemen e-government were:

- The Yemeni government need of implementation of e-government project, information sharing between the e-government organizations and trying to find the appropriate e-government framework to enhance the economical growth and provide the people with the best and fastest services offered by this new technology, By examining the e-government literature, it was found that there was a lack of research that can assist in evaluating the e-government situation in the Republic of Yemen (Alsohybe, 2007).
- According to (Alsohybe, 2007), the challenges face the Government of Yemen is trust of the Yemeni citizens and organizations to exchange information. In Yemen the results revealed that 85% of the participants think that security will be a major problem along the road of e-government implementation. Most participants do not trust online

transaction and transfer of important personal and organizational information. And

- Easy access and ability to influence managements of the government organizations in testing the model and contribute in the validity process.

3.5 Research Methods

This study used mixed method research approaches to collect the needed data. The case study approach was used, which is considered both qualitative and quantities approach, to developing mathematical model and investigation by use case study that is Yemen. For the purpose of this study, the researcher will use the main tool of the collection data process which is the distribution of survey questionnaire and qualitative interviews.

The questionnaire can be filled out at the convenience of respondents without interviewer bias or error. The main difficulty in using a questionnaire is securing high response rate (Punch, 2003). Creswell (2003) suggests a following up approach to avoid such situations, such as sending an email for reminding, or following up by phone calls. Survey can be used to find common patterns and

relationships in a large number of organisations, providing generalisable results (Gable 1994; Jick 1979). Qualitative research is a widely used method in information systems research (Benbasat et al., 1987; Walsham, 1995; Walsham, 2006).

The objective of the survey questionnaires was to apply the mathematical model and its verification; which illustrate the effectiveness of the proposed approach for the evaluation of security readiness and addressing the security requirements for the implementation of e-government in the Yemen's organizations. In addition, identify the security challenges that influence the Implementation of e-government initiatives in the government of Yemen. Interviews with review of documents will be used to reconfirm the quantitative findings in more detail. The format of the questions was open-close-ended questions. The delivery questionnaires were collected from self Administered questionnaires and interview administered, that mean the questionnaires were hand delivered to participants in each ministry with a short explanation of the questionnaire procedures and items, in addition qualitative questions will be asked of the participants in semi-structured interviews; this will ensure richness of data by giving participants time to explain their views about mathematical model and send by e-mail. The

survey questionnaire was designed according to survey form in chapter four, section (4-4); it was divided into four sections: The first section covers the respondent's specifications questionnaire. The second section covers the organization's specifications questionnaire. The third section covers the information security factors according the multi-layer model layers. Each question for model factors is given in (a) Factors measure for the practical use in the organization, three levels of indication are given "Yes, No and I Don't Know". (b) Factor Importance, are five levels of relative importance given" Critical, Major, Moderate, Minor and Not at all". The fourth section covers the security challenges.

Finally, Review of secondary resources was used in this study to develop mathematical method for the multi-layer model. Related research papers, journals, studies, and surveys were researched, collected, indexed, and reviewed by the researcher. The objective of this step was to have a good repository of all journals and conference proceeds addressing the topic of information security models, mathematical method for e-government security assessment and identify needs, and the different security methods which other researches discussed in the past.

3.6 Data collection Process

3.6.1 Sample Selection

According to Graziano and Raulin (1997) it is not possible to collect and gain data from all the available sources to solve the research problems and to find the solutions. Therefore it is recommended that from the available population, smaller units should be taken to gather data. These smaller units are referred as sample. Sampling techniques give us methods that help to reduce the amount of data needed to collect by considering only data from a sub-group rather than all possible cases or elements (Saunders & Thornhill, 2000). There are a number of ways to choose a sample for case studies (Yin, 1994). Judgmental sampling facilitates to use judgment to select cases that will enable to answer research questions and meeting objectives (Saunders,2000). To work with small samples, as in case study, where cases are selected being informative, judgmental sampling is often used (Saunders,2000).According to Maxwell(1996), “purposeful sampling” in which particular settings, persons, or events are selected deliberately in order to provide information, which cannot be provided as well from other choices, the main instrument of the data collection process is the distribution of survey questionnaire (APPENDIX A) were distribution to different Information security

specialists as a “purposeful sampling” from each of the five ministries as a governmental organizations (APPENDIX B). The choice of organizations for this research was derived from the field experiment that was conducted at the beginning of the research to examine the validity of the data collection instrument and to modify the questionnaires. This choice of ministries was based on the objective of the survey questionnaires. The sample of ministries was based on how these ministries contribute to the implementation of e-government in Yemen, (a) the size of the ministries to include small and large ministries, (b) the level of IT use, (c) the type of e-services they provide to the public and (d) ministries willingness to participate in this research and allow the researcher to conduct interviews and surveys by their facilities.

The totals of 17 individuals were selected from five ministries for the survey questionnaire of this research. The selection subjects of survey questionnaire according to Maxwell (1996) was the result of “purposeful sampling” in which particular settings, persons, or events are selected deliberately in order to provide information, which cannot be provided as well from other choices. The survey questionnaire sample was “IT Manager, information Security Manager, information Security Consultant, and information Security Specialist”.The survey questionnaire was

distributed to these individuals. 20 of the questionnaires that were distributed, only 18 questionnaires were returned, and used for the analysis for this research, which represent about 90% response rate. Questionnaires were examined for missing data and questionnaires with less than 50% of the questions answered were omitted because of the missing data. The number of the cancelled questionnaires was only one. and 17 are valid questionnaires for analysis that means about 86% of the total distributed surveys. The information from these questionnaires was used for analysis in this research using the statistical package for social sciences (SPSS) and Ms Excel.

3.7 Data Analysis

The data analysis method began by coding the collected information. Then the data analysis strategy involved the use of software's such as SPSS and Ms Excel to help analysis and display the collected information. The use of SPSS and Ms Excel programs assist in coding and analysis process of the collected data from the survey questionnaires. The use of frequency tables, charts and graphs to present the findings in an understandable manner required use of computer programs. A detail discussion and analysis will follow to provide reader with the information

needed such as percentages, frequency of occurrence and other findings related to the research in chapter five.

3.8 Research Validity

According to Robson (2002), Validity is the degree to which what is observed or measured is the same as what was purported to be observed or measured. At its most simple, this refers to the truth status of research reports. However, a great variety of techniques for establishing the validity of measuring devices and research designs has been established, both for quantitative and for qualitative research. More broadly, the status of research as truth is the subject of considerable philosophical controversy. Triangulation is appropriate in qualitative research in increasing the study's validity. The triangulation also enhances overall validity, as the multiple lines of evidence obtained during data collection converge to a common conclusion. This methodological triangulation illuminates or nullifies some extraneous influences encountered during data collection (Stake, 1995; Miles &Huberman, 1994; Robson, 2002).

The main issue related to validity is the results of applying the mathematical model and give real indicators also increasing the study's validity, and to ensure validity of the mathematical model Since Yemen

was taken as a case study, the model was delivery to security managers of Yemen government organizations for verification and Validation. The model was evaluated by the Yemeni's government security team, consultants, and was found to be applicable to the current needs of the government organizations. It was advisable as the participants should be part of the e-government initiative. The validation process evaluated the mathematical model and its usability. It also included a form for questionnaire, based on the model, for self assessment of security readiness indicators, by government organizations wishing to enhance their information security.

To ensure validity of the data collection tool which in this case was survey questionnaires of pilot test, and was used to makes sure that these instruments capture what they intended to. A pilot test is a small version of the final experiment or test of the data collection instrument (Robson, 2002) which in this case the survey questionnaire. Yin (1994) views the pilot test as a helping method to refine the data collection plans with respect to the content of the data and the procedures of data collection. For the purpose of this research, a pilot test was performed to 6 participants from information security specialists, the instrument was modified accordingly as it is in (APPENDIX A). Another issue related to validity

was the survey questioners were advised by three professors “IT, Statistical, information security” and selecting a large sample for studies about 16% from Yemeni’s ministries.

Finally, the issue related to validity is the language of the tool, as mentioned in the research that was conducted in Yemen, and uses Arabic as the main language of the country. Therefore, the tool was developed to take into consideration differences of meaning between Arabic and English. Further to, there was an attempt to minimize the problem of lack of equivalence between the Arabic and English version of the instruments.

3.9 Summary

This chapter provides full explanation of the research design to the developing of the mathematical model and validity by using case study that is Yemen e-government. The survey questionnaires were modified using the feedback from the pilot tests conducted for the same purpose. The research methods contained survey questionnaire (APPENDIX A). Qualitative and quantitative used to gather for analyze information which was used to answer the research questions from five ministries where it represent almost 16% of the total ministries in Yemen.

Chapter four

The Mathematical Model

4.1 Introduction

This chapter is concerned with development of the mathematical model, according to multi-layer model (Alazazi, 2008), and based on Al-Rabiah (2007), Al-Osaimi (2007), Al-Osaimi, AL-heraish and Bakry (2008) methods because there were help to achieve research objects, appropriate for multi-layer model architecture, work with other models effectually and a modern. The model is presented in the following three sections: The first section(4.2) is concerned with identifying the Multi-Layer model structure; The second section(4.3) is associated with describing how it can be investigated; while The third section(4.4) is related to provide investigation steps to the model on the application the practical case-study.

4.2 The Model Structure

The Multi-Layer models consist of "47" factors have involved

in the following five main layers:" technology, policy, Operational and management, Competencies, and decision make layer". The Multi-Layer structure is illustrated in figure4-1(a), (b). The Table integrates the factors of the model over the model layers.

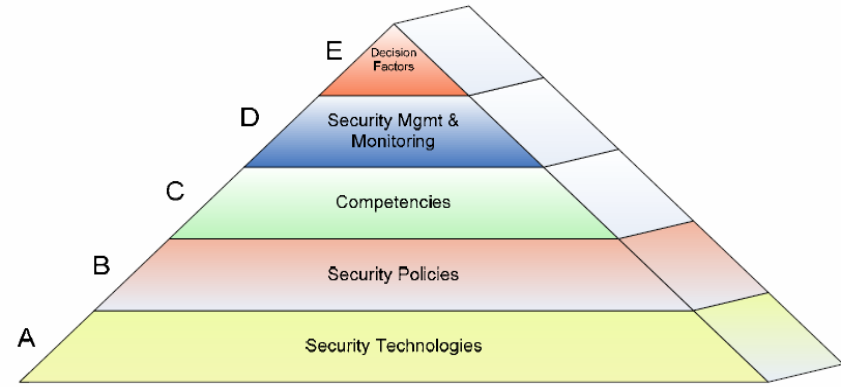

Figure 4-1(a): the Multi–layer model layers: (Alazazi, s., 2008).

	Sub-layer (factors)		Sub-layer (factors)	
Technology	Access Control	A1	Intrusion Detection and Prevention	A2
	Anti Virus and Malicious Code	A3	Authentication and Passwords	A4
	Files and Integrity Check	A5	Cryptography	A6
	VPN	A7	Vulnerability Scanning Tools	A8
	Digital Signatures and Certificates	A9	Biometrics	A10
	Logical Access Control (Firewalls)	A11	Security Protocol	A12
Policies	Password Management	B1	Log-in Process	B2
	Logs Handling	B3	Computer Viruses	B4
	Intellectual Property Rights	B5	Data Privacy	B6
	Privilege Control	B7	Data Confidentiality	B8
	Data Integrity	B9	Internet Connectivity	B10
	Administrative Policies	B11	Encryption Policies	B12
	HR Security Policies	B13	Third Party Policies	B14
	Physical Security Policies	B15	Operation Security Policies	B16
Competencies	Security Operation and management	C1	Security Architecture and development	C2
	Ethical Hacking	C3	Security Policies and development	C4
	Computer Forensics	C5	Cryptography	C6

	Security Programming	C7	Laws and regulation	C8
	Security Implementation and Configuration	C9	Security Analysis	C10
OPS mgmt	Operational Policies and Procedures	D1	Management Tools	D2
	Correlation and data mining	D3	Reporting and Response	D4
	Analysis and Human intervention			D5
Decision	Cost	E1	Awareness	E2
	Need	E3	Technologies Availability	E4

Figure 4-1(b): the Multi–layer model factors: (Alazazi, s., 2008).

4.3 Investigation method

The researcher suggests that the development of a mathematical method for analysis and readiness assessment based in multi-layer model to be consisted of three main levels:

- The top level is the model level, which provides a single s-readiness indicator that integrates indicators of its five layers.
- The layer level, has five layers which provides an indicator for each layer integrating the indicators of its assessment factors; and
- The bottom level is the factor levels, which has "47 factors" distributed over the five layers, and provide an indicator for each factor.

Investigation of the model, is described below which provides evaluation indicators for each of the model layers and in accumulating the factor indicators from one layer; it assigns weights to the values of the indicators, so each indicator is valued according to its importance and information security of the considered organization. The results of the main layers can be represented by a single value for multi-layers model; this can be called the security readiness indicator of the e-government. The assessment starts at the bottom level, where each “factor” is "measured/graded”, and assigned a "weight" relative to its estimated effect on the considered case study, then steps up to higher levels assessing “layers”, and the “top level”. In table 4-1 each of the five model layers and factors were indexed, were associated with a measure and with a weight. Each main layer can be evaluated independently using factors associated with it. Individual results for the main layers can be presenting graphically by a radar graph.

Table 4-1: model layer and factor index

Model LEVEL					
Main layer	Technology	Policies	Competencies	Op&Mag	Decision
INDEX	i = 1	i =	i = 3	i = 4	i = 5
MEASURE	*M[1]*	*M[2]*	*M[3]*	*M[4]*	*M[5*
WEIGHT	*w[1]*	*w[2*	*w[3]*	*w[4]*	*w[5]*
LAYER LEVEL					
LAYER	Any of the five main layer, identified as: l [i]				
INDEX	i : the layer index: $1 \leq i \leq 5$				

	j_i represents the factor index of layer i: $1 \le j_i \le J_i$ (j_i: number of factors in layer i)
MEASURE	$M[i, j_i]$
WEIGHT	$w[i, j_i]$

The description of these three levels is as follow:

- **Firstly**, the bottom level is concerned with the factors, which has "47 factors" distributed over five layers, which provides an indicator for each factor according to the following steps:

1) Calculate factor measures and factor importance from survey questions results (assessment form).
2) Calculate factor weight according to the equation (1):

$$\text{Factor weight} = \frac{\text{Factor importance}}{\sum_{ji=1}^{ji=\,Ji} \text{Factor importance}} \qquad \textbf{(1)}$$

$$i: \text{layer index}: 1 \le i \le 5$$
$$ji: \text{number of factors in layer}(i)$$

3) Calculate factor Relative Weighted Indicator according to the equation (2):

$$\text{Factor Relative Weighted Indicator} = \text{Factor measure} \times \text{Factor weight} = \mathrm{M}[i, ji] \times W[i, ji] \quad \textbf{(2)}$$

- **Secondly,** this level is concerned with the layers. It shows how the indicators of this layer can be found. The evaluation of these indicators depends on the evaluation of the indicators of factors. Relative weights are also taken into account, with respect to the relationships of model factors with their related model layers. It is shown in the following steps:

  1) Calculate the layer importance from survey questions results.
  2) Calculate the layer measure from Factor Relative Weighted Indicator according to the equation (3):

$$\text{Layer measure} = \sum_{ji=1}^{ji=\,Ji} \mathrm{M}[i, ji] \times W[i, ji] \quad \textbf{(3)}$$

$$i: \text{the layer index}: 1 \le i \le 5$$

$$ji: \text{number of factors in layer}(i): 1 \le ji \le Ji$$

The equations for all model layers are:

$$\text{Technology measure} = \sum_{j1=1}^{j1=\,J1} \mathrm{M}[1, j1] \times W[1, j1] \quad \textbf{(3a)}$$

$$\text{Policies measure} = \sum_{j2=1}^{j2=J2} M[2, j2] \times W[2, j2] \quad \textbf{(3b)}$$

$$\text{Competencies measure} = \sum_{j3=1}^{j3=J3} M[3, j3] \times W[3, j3] \quad \textbf{(3c)}$$

$$\text{Org \& Mag measure} = \sum_{j4=1}^{j4=J4} M[4, j4] \times W[4, j4] \quad \textbf{(3d)}$$

$$\text{Decision measure} = \sum_{j5=1}^{j5=J5} M[5, j5] \times W[5, j5] \quad \textbf{(3e)}$$

3) Calculate the layer weight according to the equation (4):

$$\text{Layer weight} = \frac{\text{Layer importance}}{\sum_{i=1}^{i=5} \text{Layer importance}} \quad \textbf{(4)}$$

$$i: \text{layer index}: 1 \le i \le 5$$

4) Calculate the layer Relative Weighted Indicator according to the equation (5):

$$\text{Layer Relative Weighted Indicator} = \text{Layer wieght} \times \text{Layer measure} = M[i] \times W[i] \quad (5)$$

5) Individual results for the Factors can be graphically integrated

by a “radar graph” main layer would have its own “radar graph”.

- **Finally**, the top level is concerned with the overall indicator of all model layers, and putting together collectively, that is the indicator of security readiness for e-government (s-readiness). The evaluation of this indicator depends on the evaluation the indicators of the five model layers. The relative weights of these indicators are taken into account. it is shown in the following steps:

  1) Calculate overall indicator of all model layers s-readiness according to the equations (6):

$$\text{Security readiness indicator} = \sum_{i=1}^{i=5} \mathrm{M}[\mathrm{i}] \times W[i] \qquad \textbf{(6)}$$

  2) Overall result for the Model can be graphically integrated by a radar graph.

4.4 Practical Assessment Form (Survey Form)

The above model enables practical assessment of security readiness of e-government, with help of a multi-layer model. These investigations would produce indicators of this readiness at various layers of the multi-layers model structure. This would help diagnosing strengths and

weaknesses of the information security management in the government organizations; and would also help directing their effort toward the factors that will require improvements.

In the application of the model to practical case-study would require design of a comprehensive assessment form (survey form), or questionnaire (survey questionnaire form).

Before, describes the basic components of the assessment (survey form), this some issues are taken into account:

- The form should cover five layers, and factors of the model.
- For every measure concerned with the evaluation of factor has two inputs to be specified: the measure is practically applied; and the relative weight of this measure, is in regards to accomplishing the factors considered
- For evaluation of the achievement of layers, the status of their factors would be needed as an input. Another needed input value is the relative weight of each security factor involved in the achievement of the layers.

The main components of the investigation form (survey form) are described as follows:

- Determine the grades for evaluation of the measures and grade for

important level. The Table 4-2 (a) gives an example for the evaluated measures grades; it suggests uses of three grades for evaluation of the measures. Table 4-2 (b) gives an example of important level grades; it suggests using of five grades for important level.

. Table 4-2 (a) grades for the evaluated measures

1	2	3
Yes	No	I don't

Table 4-2 (b): grades for important level.

1	2	3	4	5
Not at all	Mino	Moderate	Major	Critical

- The main model factors associated with the layer; the above components are given in the following Tables for each multi- layer model layers. Table 4-3 (a) introduces the multi- layer model part concerned with the technology layer, which has "12" factors.

Table 4-3 (a): The Technology layer

Factor
Access Control
Intrusion Detection and Prevention
Anti-Virus & Malicious Code
Authentication and Passwords
Files Integrity Checks
Cryptography
VPN
Vulnerability Scanning Tools
Digital Signatures and Certificates
Biometrics
Logical Access Control (Firewalls)
Security Protocols

- Table 4-3 (b) presents the "second" main parts of the model associated with the policy layer, which has "16" factors.

Table 4-3 (b): the policy layer

Factor
Password Management
Log-in Process
Logs Handling
Computer Viruses
Intellectual Property Rights
Data Privacy
Privilege Control
Data Confidentiality
Data Integrity
Internet Connectivity
Administrative Policies
Encryption Policies
HR Security Policies
Third Party Policies
Physical Security Policies
Operation Security Policies

- Table 4-3 (c) presents the "third" main parts of the model associated with the Operational and management layer, which has "10" factors.

Table 4-3 (c) the Operational and management layer,

Factor
Security Operation and management
Security Architecture and development
Ethical Hacking
Security policies and development
Computer Forensics
Cryptography
Security Programming
Laws and regulations
Security implementation and configuration
Security Analysis

- Table 4-3 (d) presents the "four" main parts of the model associated with the Competencies layer, which has "5" factors.

Table 4-3 (d): the Competencies layer

Factor
Operational Policies and procedures
Management Tools
Correlation and data mining
Reporting and Response
Analysis and human intervention

- Table 4-3 (e) presents the "four" main parts of the model associated with the decision make layer, which has "4" factors

Table 4-3 (e): the decision make layer

Factor
Cost
Awareness
Need
Technologies Availability

Table 4-4 provides examples of how the relative weights of three measures can be assigned, and how status of their factor can be determined. In addition figure 4-2 shows the radar graph of layer considered in this example.

Table 4-4: the layer result in example

Factor	Measure	Importance	Weight	Relative Weighted Indicator
Access Control	2	3.6	0.08	0.16
Intrusion Detection and Prevention	1.3	4	0.09	0.12
Anti-Virus & Malicious Code	2	4	0.09	0.18
Authentication and Passwords	2	4	0.09	0.18
Files Integrity Checks	0	2.6	0.06	0
Cryptography	0.6	3.6	0.08	0.05
VPN	0.6	4	0.09	0.06
Vulnerability Scanning Tools	0.6	3.6	0.08	0.05
Digital Signatures and Certificates	0	3.3	0.07	0
Biometrics	0.6	3	0.06	0.04
Logical Access Control (Firewalls)	2	4	0.09	0.18
Security Protocols	0.6	4	0.09	0.06
TECHNOLOGY *measure*				1.1

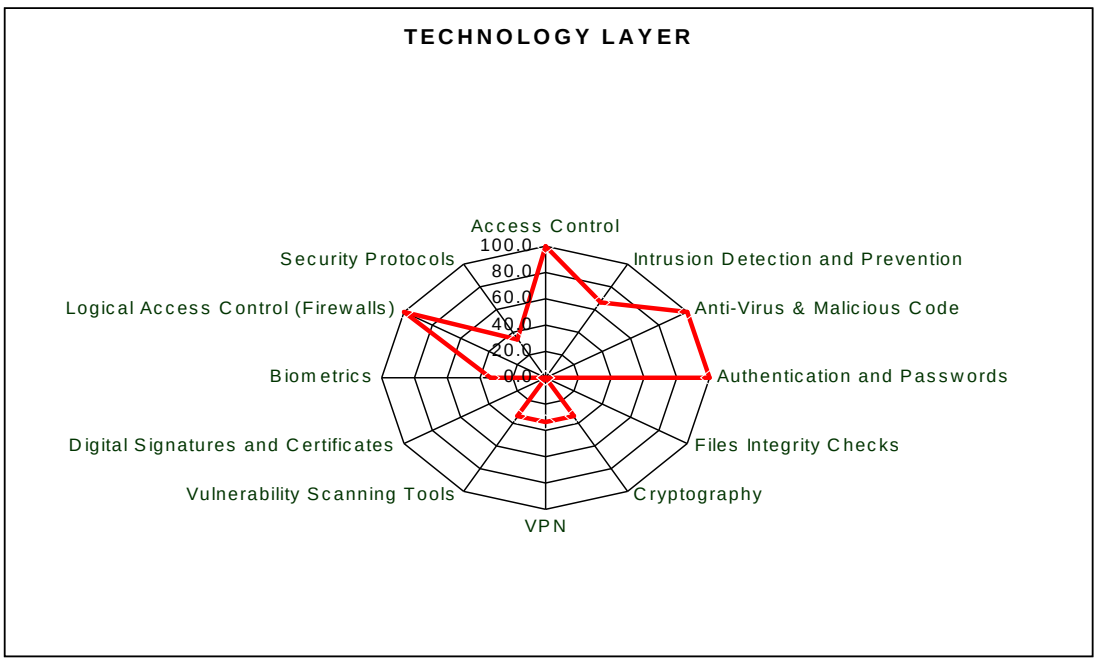

Figure 4-2: The layer radar graph in example

4.5 Summary

The work presented in this chapter presents the steps to make Multi-layer mathematical model which is the first objective of the thesis. It is concerned with the development of the mathematical model that Provides security readiness indicators based on the multi-layer model factors. It gives an integrated view of the model, with illustrations of how to provide indicators, for the evaluation of information security readiness, according to the multi-layer model. And it provides useful tools for the assessment information security readiness for e-government. The assessment form associated with the model show how the assessment can be conducted, and how results can be derived and presented.

CHAPTER FIVE

DATA ANALYSIS AND DISCUSSION

5.1 Introduction

Purpose of this chapter is to present and analyze the research data which obtained by means of the questionnaire (Appendix A) and used during the survey. The data was analyzed and interpreted to address the research questions, as well as the determined in chapter one. This chapter describes the data analysis process used to interpret the data collected during the months of August through September 2010, using survey questionnaires as the data collection instruments. This chapter is organized as follow: The first section describes the respondent's and organization specifications (Sample characteristics). The second section describes findings of the survey questionnaires which includes answers to the three research questions

5.2 Characteristics of the Survey Questionnaires

Before starting analysis of the survey questionnaires we have to mention that the data collection procedure conformed to the guidelines recommended by Robson (2002), Cooper and Schindler (2003) and Miles and Huberman (1994). As mentioned in the methodology section, these procedures included the use of cover letter explaining content of the questionnaire and purpose of the research. The totals of 17 individuals were selected from five ministries for the survey questionnaire of this research. Selection of survey questionnaire sample was deliberately in order to provide information, which cannot be provided from other choices as well. The survey questionnaire sample is Security Specialists in government organizations. The survey questionnaire was distributed to these individuals. About 20 of the questionnaires were distributed; only 18 questionnaires were returned and were used for the analysis for this research, which represent about 90% response rate. Questionnaires were examined for missing data and questionnaires with less than 50% of answered questions were omitted because of the missing data. And number of the cancelled questionnaires was just one and we set with 17 valid questionnaires for analysis which is about 86% of the total distributed surveys. These questionnaires gave a clear overview of the

security current status for e-government in these ministries. Table 5-3 provides the personal information collected by the above questionnaire. The Table gives full details for the position of the participants whom provided the data, his IS/IT experience, age, degree, field of study, & special, and academic qualification.

Table 5-1: the participants' Personal Characteristics

	characteristics	Frequency	percentage
1	**Age?**		
	Under25 years		0
	25-40 years	**17**	100 %
	41-50 years		0
	51-60 years		0
	Over 60 years		0
2	**Academic qualifications**		
	High School-Diploma or less.		0
	Bachelor.	**16**	94 %
	Master.	**1**	6 %
	Doctorate		0
	Other		0
3	**Field of study**		
	Computer Science	**7**	41 %
	Engineering	**10**	59 %
	Management		0
	Business		0
	Other		0
4	**Special qualifications in Information Security**		
	CIW		0
	CISSP		0
	SANS		0
	Other	**2**	12 %
5	**Position**		

	Information Security Manager	**3**	18 %
	Information Technology Manager	**5**	29 %
	Consultant.	**1**	6 %
	Other	**6**	35 %
6	**Experience on IS/IT**		
	Under 6 Months		0
	7-12 Months		0
	13-18 Months	**3**	18 %
	19-24 Months		0
	Over 25 Months	**14**	82 %

From the above table we can see that all of respondents are between 25-40 years ages, most majority of these employees held a bachelor degree that is 94%,and only 6% had a master degree, 12% have special qualification on IT, 82% of them have an experience for more than 2 years in information security and information technology. 59% with engineering degrees, 41% with degree in computer science. additionally, 47% of the respondents are at manager level and 6% with Consultant.

5.3 Characteristics of the Survey organizations

Table 5-2 provides the collected data of the five organizations in Yemen included in the study. The Table gives full details of the size, organization experience, separation of information security department, e-services type, and the field of each selected organization in the study.

Table 5-2: organizations Characteristics

	characteristics	**Frequency**	percentage
1	**Type**		
	public	**17**	100 %
	privet		
2	**Size: No. Employees**		
	Less than 100		0
	100 to 500	**13**	76 %
	501-1000		0
	1001 to 3000		0
	Over 3000	**4**	24 %
3	**Field**		
	Government	**17**	100 %
	other	**0**	0
4	**Business Experience**		
	Under 12 Months		0
	13-24 Months		0
	Over 24 Months	**17**	100 %
5	**Separate IS Dep**		
	Yes	**6**	35 %
	No	**11**	65 %
6	**Size: No. Computers**		
	Less than 100		0
	100 to 500	**13**	76 %
	501-1000	**4**	24 %
	1001 to 3000		0
	Over 3000		0
7	**e-services type**		
	Information publishing	**13**	76 %
	one way interactive e-service.		0
	Two-Way Interactive e-services.	**4**	24 %
	A transactional e-service.		0
	Combination of all the above.		0

Based on the information provided in Table 5-2, we can see that the questionnaire have been answered by the following business fields: 100% governmental organizations, All of them have been in business for more than two years .so, 35% of them have separate information security department, 24% have tow-way interactive e-services,76% have Information publishing,76% have between 100 to 500 Employees, 24% have over 3000 Employees, 76% have 100 to 500 computer, and 24% have between 501 to 1000 computer.

Question one: What are the assessment security readiness indicators for implementing of e-government in Yemen organizations?

5.3 Results of the Technology Layer

First, the survey questionnaires focused on several factor such as the Access Control, Intrusion Detection& Prevention, Anti-Virus & Malicious Codes Scanners, Authentication& Passwords, Files Integrity Checks, Cryptography, VPN, Vulnerability Scanning Tools, Digital Signature & Digital Certificates, Logical Access Control (Firewalls), and Security Protocols.

Table 5-3 summarizes some of the information which was collected from the survey questionnaires, that reflects the current state of information security technologies usage in the organizations of Yemen.

Table 5-3: current state results of the Technology Layer

Factor	**Indicator average-Measure**	**Importance average**	**Weight**	**Relative Weighted Indicator**
Access Control	2.00	3.67	0.08	0.17
Intrusion Detection and Prevention	1.33	4.00	0.09	0.12
Anti-Virus & Malicious Code	2.00	4.00	0.09	0.18
Authentication and Passwords	2.00	4.00	0.09	0.18
Files Integrity Checks	0.00	2.67	0.06	0.00
Cryptography	0.67	3.67	0.08	0.06
VPN	0.67	4.00	0.09	0.06
Vulnerability Scanning Tools	0.67	3.67	0.08	0.06
Digital Signatures and Certificates	0.00	3.33	0.08	0.00
Biometrics	0.67	3.00	0.07	0.05
Logical Access Control (Firewalls)	2.00	4.00	0.09	0.18
Security Protocols	0.67	4.00	0.09	0.06
Technology layer Measure				1.1

Each main layer has been illustrated in a radar graph to indicate Strengths and weaknesses as shown in Figure 5-1 for Technology layer.

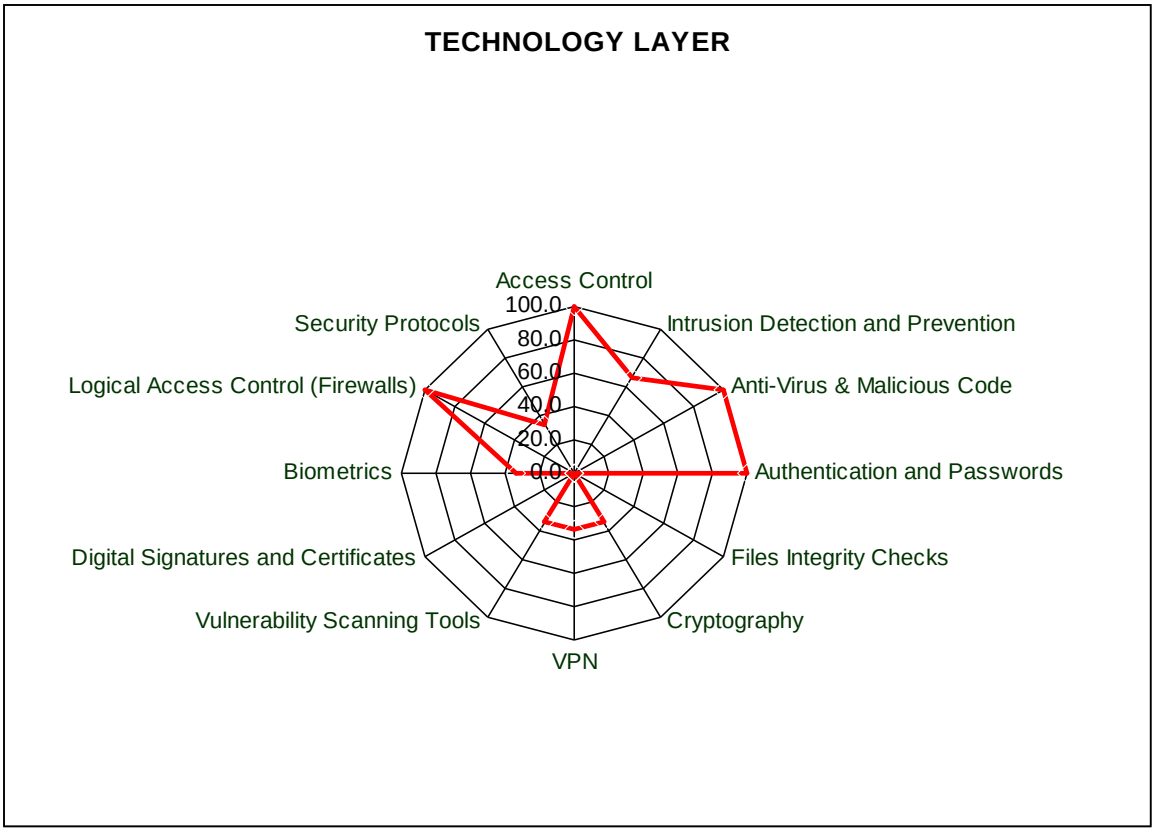

Figure 5-1: the radar graph of Technology results

From figure 5-1 the assessment indictors for technology layer are illustrated in the following: the Access Control with 100%, 67 % with Intrusion Detection & Prevention ,Anti-Virus & Malicious Codes Scanners with 100%,Authentication & Passwords with 100%,Files Integrity Checks with 0%,Cryptography with 33%,VPN with 33%,Vulnerability Scanning Tools with 33%,Digital Signature and Digital Certificates with 0 %,Biometrics with 33%, Logical Access Control (Firewalls) with 100% and Security Protocols with 33%.

5.4 Results of the Policy layer

secondly, the survey questionnaires focused on several factor such as Password management ,Login process, Logs handling, Computer viruses , Intellectual property rights, Data privacy, Privilege control, confidentiality, Data integrity, Internet connectivity , policies , Encryption policies , HR security policies , Third party policies , Physical security policies, Operation security policies.

Table 5-4 summarizes some of the information which was collected from the survey questionnaires, that reflects the current state of information security policies usage in the organizations of Yemen.

Table 5-4: current state results of the Policy layer

Factor	Indicator average Measure	Importance average	Weight	Relative Weighted Indicator
Password Management	0.67	3.00	0.05	0.04
Log-in Process	2.00	3.67	0.06	0.13
Logs Handling	0.67	2.67	0.05	0.03
Computer Viruses	0.67	3.33	0.06	0.04
Intellectual Property Rights	0.67	3.00	0.05	0.04
Data Privacy	0.67	4.00	0.07	0.05
Privilege Control	0.67	3.67	0.06	0.04
Data Confidentiality	0.67	3.67	0.06	0.04
Data Integrity	0.67	4.00	0.07	0.05
Internet Connectivity	0.67	4.00	0.07	0.05
Administrative Policies	0.67	3.67	0.06	0.04
Encryption Policies	0.67	3.67	0.06	0.04

HR Security Policies	0.67	3.67	0.06	0.04
Third Party Policies	0.67	3.00	0.05	0.04
Physical Security Policies	0.67	3.67	0.06	0.04
Operation Security Policies	0.67	4.00	0.07	0.05
Policies layer Measure				0.8

Policy layer constructed from 16 factors shown and their scores in Figure 5-2.

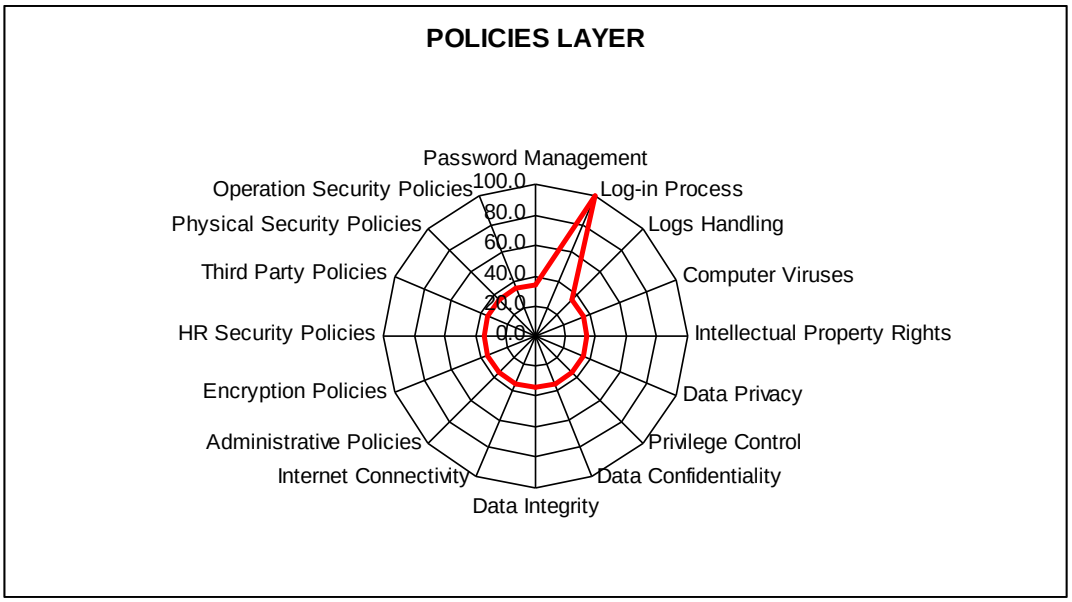

Figure 5.2: the radar graph of Policy layer

From Figure 5-2 the assessment indictors for Policy layer are illustrated in the following: only the Log-in Process with 100 %, but 33% with other factors in this layer.

5.5 Results of the Competencies Layer

Third, the survey questionnaires focused on several factor such as Security Operation and management, Security Architecture and development, Ethical Hacking, Security policies and development, Computer Forensics, Cryptography, Security Programming, Laws and regulations, Security implementation and configuration and Security Analysis's.

Table 5-5 summarizes some of the information which was collected from the survey questionnaires, that reflects the current state of information security Competencies usage in the organizations of Yemen.

Table 5-5: current state results of the Competencies layer

Factor	Indicator average Measure	Importance average	Weight	Relative Weighted Indicator
Security Operation and management	0.67	3.67	0.12	0.08
Security Architecture and development	0.67	3.67	0.12	0.08
Ethical Hacking	0.67	3.67	0.12	0.08
Security policies and development	0.67	3.67	0.12	0.08
Computer Forensics	0.00	3.00	0.09	0.00
Cryptography	0.00	3.33	0.11	0.00
Security Programming	0.00	3.00	0.09	0.00

Laws and regulations	0.67	2.67	0.08	0.06
Security implementation and configuration	0.67	2.33	0.07	0.05
Security Analysis	0.67	2.67	0.08	0.06
Competencies layer Measure				0.5

the Competencies layer are shown in Figure 5-3.

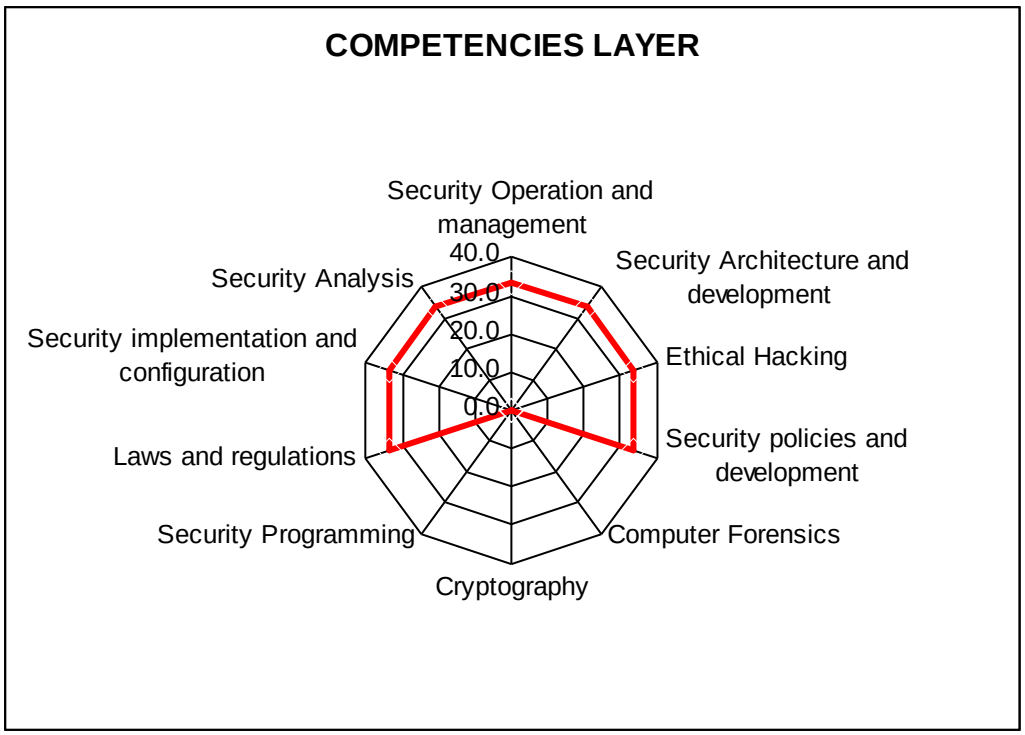

Figure 5-3: the radar graph of Competencies results.

From Figure 5-3 the assessment indictors for Competencies layer are illustrated in the following: 33% with Security Operation and management, Security Architecture and development, Ethical Hacking, Security policies and development, Laws and regulations, Security

implementation and configuration and Security Analysis's but 0 % with Computer Forensics, Cryptography and Security Programming.

5.6 Results of the Operations and Management Layer

Fourth, the survey questionnaires focused on several factor such as Operational Policies and procedures, Management Tools, Correlation and data mining, Reporting and Response and Analysis and human intervention.

Table 5-6 summarizes some of the information which was collected from the survey questionnaires, that reflects the current state of information security Operations and Management usage in the organizations of Yemen.

Table 5-6: current state results of the Operations and Management layer

Factor	Indicator average Measure	Importance average	Weight	Relative Weighted Indicator
Operational Policies and procedures	0.67	3.00	0.18	0.12
Management Tools	0.67	3.00	0.18	0.12
Correlation and data mining	0.67	3.00	0.18	0.12
Reporting and Response	1.33	3.67	0.22	0.30

Analysis and human intervention	0.00	3.67	0.22	0.00
Operations And Management Layer Measure				0.7

Operations And Management layer constructed from five factors shown and their scores in Figure 5-4

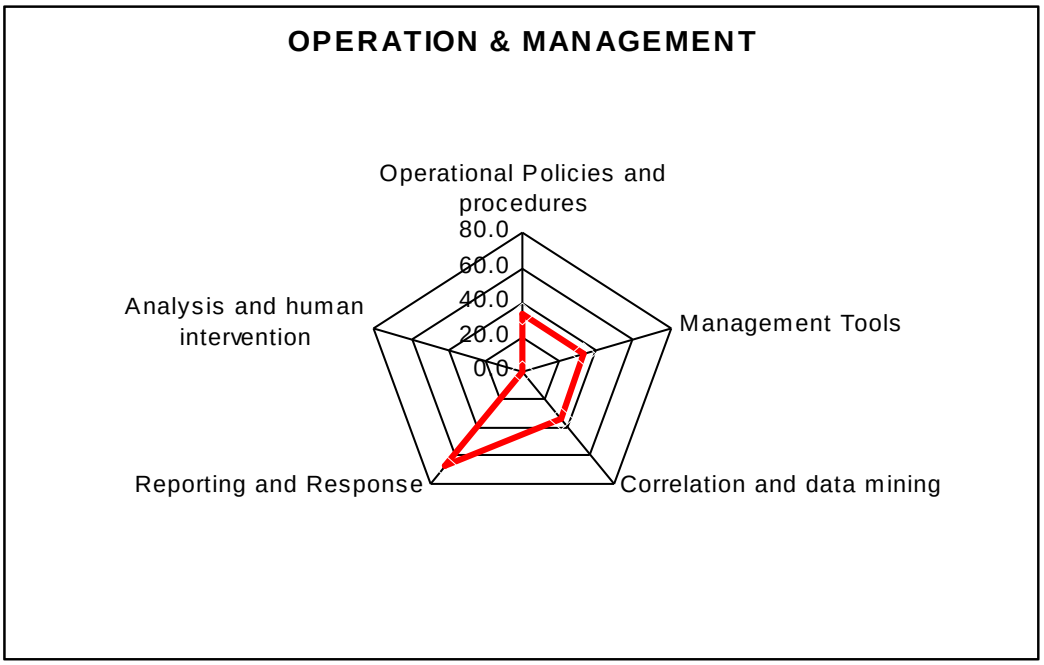

Figure 5-4: the radar graph of Operations and Management layer results.

From Figure 5-4 the assessment indictors for Operations and Management layer are illustrated in the following: 33% with the Operational Policies and procedures, 33% with Management Tools, 33% with Correlation and data mining, 67% with Reporting and Response and 0% with Analysis and human intervention.

5.7 Results of the Decision Layer

Fifth, the survey questionnaires focused on several factors will assist in reaching the decision for selecting or considering a security technology, policy, operational procedure, or hiring a resource with certain security competency such as Cost, awareness, need, technologies availability.

Table 5-7 summarizes some of the information which was collected from the survey questionnaires, that reflects the current state of information security Decision usage in the organizations of Yemen.

Table 5-7: current state results of the Decision layer

Factor	Indicator average Measure	Importance average	Weight	Relative Weighted Indicator
Cost	1.33	2.67	0.21	0.28
Awareness	1.33	3.33	0.26	0.35
Need	2.00	4.00	0.32	0.63
Technologies Availability	1.33	2.67	0.21	0.28
Decision layer Measure				1.5

Decision layer constructed from 4 factors shown and their scores in Figure 5-5

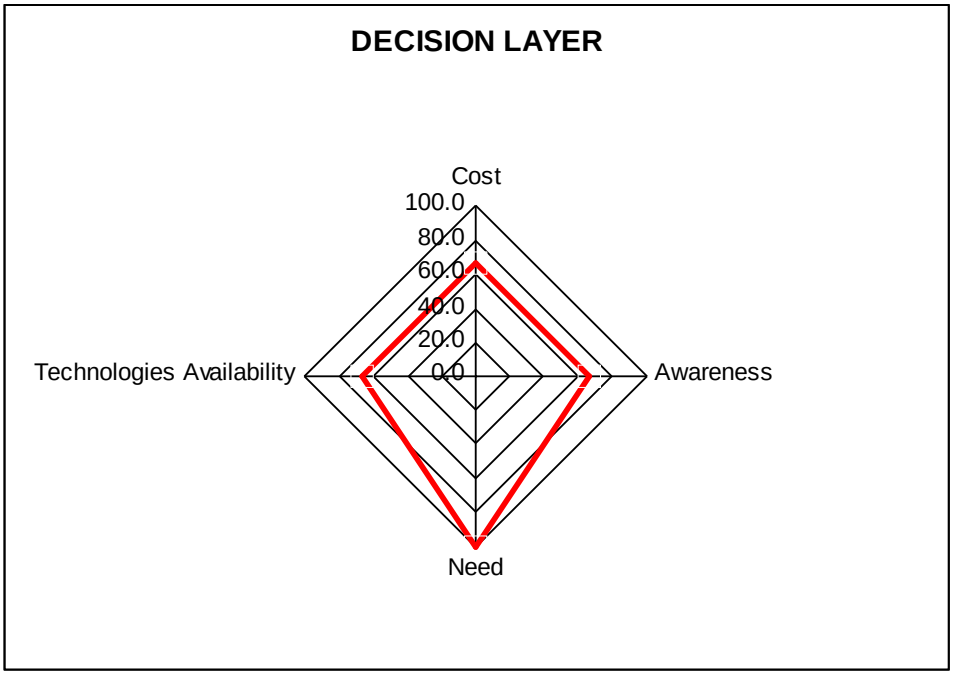

Figure 5-5: the radar graph of Decision results.

From Figure 5-5 the assessment indictors for Decision layer are illustrated in the following: 67% with the Cost, 67% with the awareness, 100% with the need and 67% with the technologies availability.

5.8 Model Overall Results

Finally, the survey questionnaires focused on main layer will assist in calculate a results for Model overall. Table 5-8 summarizes some of the information which was collected from the survey questionnaires, and reflects the current state of information security layers usage in the organizations of Yemen.

Table 5-8: Main layer results of Government Organizations

layer	Measure	Importance	Weight	Relative Weighted Indicator
TECHNOLOGY	1.11	4.00	0.21	0.23
POLICIES	0.75	4.00	0.21	0.16
COMPETENCIES	0.47	4.00	0.21	0.10
OPERATIONS AND MANAGEMENT	0.67	3.33	0.17	0.11
DECISION	1.54	4.00	0.21	0.32
Model indictor				0.7

Figure 5-6 shows the radar graph of overall results

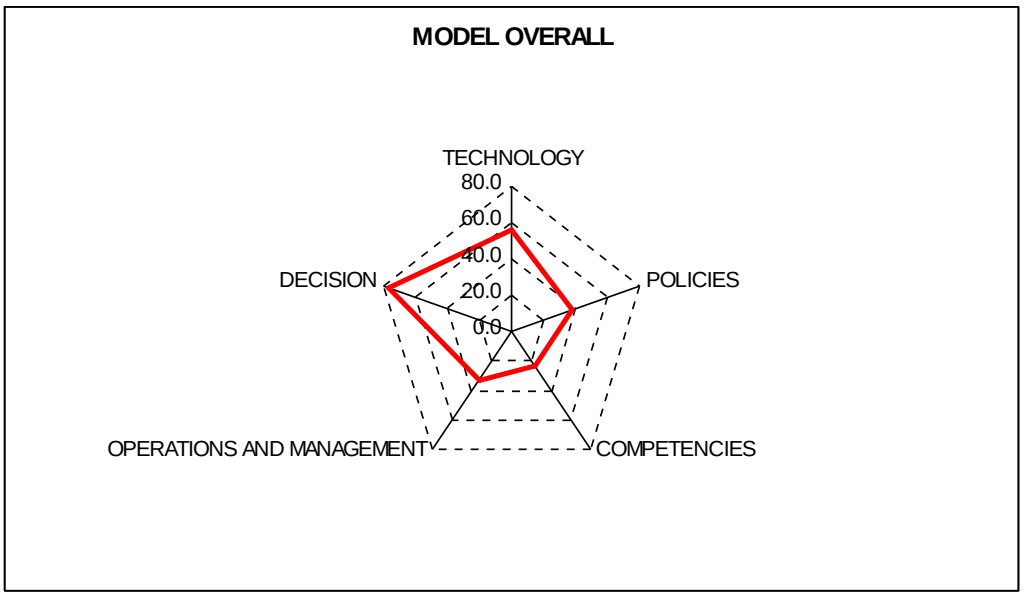

Figure 5-6: the radar graph of overall results

From Table 5-8 and Figure 5-6 calculate the Model layers results as a percentage that illustrated in table 5-9.

Table 5-9: the percentage of readiness results

layer	Score
TECHNOLOGY	56 %
POLICIES	38 %
COMPETENCIES	24 %
OPERATIONS AND MANAGEMENT	33 %
DECISION	77 %
MODEL overall	**34.3 %**

It is clear from Table 5-9 that's Decision layer has the highest score with 77%, Competencies layer has the lowest one with 24 %, 56% with Technology layer, 38% with Policies layer and 33% with Operations Management layer.

To conclude that Table 5-9 and Figure 5-6 come to have the indictor of security readiness for implementation of e-government project in Yemen is (0.7) that means government organizations achieved about 34% of the multi-layer model requirements. The assessment results of Yemen government would provide organizations with guidelines on future information security improvements.

5.9.1 Strengths and weaknesses points

In this section, we tried to list of the missing factors for Yemen government organizations based in last results. Which consider a weakness points in organization security system and source of threats or risks. So, this list was useful on future to improve the security state in organizations. The selecting of factor based on factor measure value that has less then 70%, because of Yemen is a developing country. Table 5-10 shows the weaknesses and Strengths points for Yemen government organizations based on multi-layer model.

Table 5-10: strength and weaknesses points

layer	Strength points	weaknesses points
Technology	- Access Control. - Anti-Virus & Malicious Code. - Authentication and Passwords. - Logical Access Control (Firewalls).	- Intrusion Detection and Prevention. - Files Integrity Checks. - Cryptography. - VPN. - Vulnerability Scanning Tools. - Digital Signatures and Certificates - Biometrics - Security Protocols

policy	- Log-in Process.	- Password Management - Logs Handling - Computer Viruses - Intellectual Property Rights - Data Privacy - Privilege Control - Data Confidentiality - Data Integrity - Internet Connectivity - Administrative Policies - Encryption Policies - HR Security Policies - Third Party Policies - Physical Security Policies - Operation Security Policies
COMPETENCIES		- Security Operation and management. - Security Architecture and development - Ethical Hacking - Security policies and development - Computer Forensics - Cryptography - Security Programming - Laws and regulations - Security implementation and configuration - Security Analysis
OPERATIONS AND MANAGEMENT		- Operational Policies and procedures - Management Tools - Correlation and data mining - Reporting and Response - Analysis and human intervention
DECISION	- Need	- Cost - Awareness Technologies Availability

Question tow: What are the security challenges that influence the Implementation of e-government initiatives in the government of Yemen?

5.9.2 Information security standards and challenges

- **The coexistence of information security standards in Yemen**

The results of the survey showed in figure 5-7 that 13 respondents (82%) stated that it is not have standard whilst 4 respondents (18%) answered with yes, and (0%) answered with not sure.

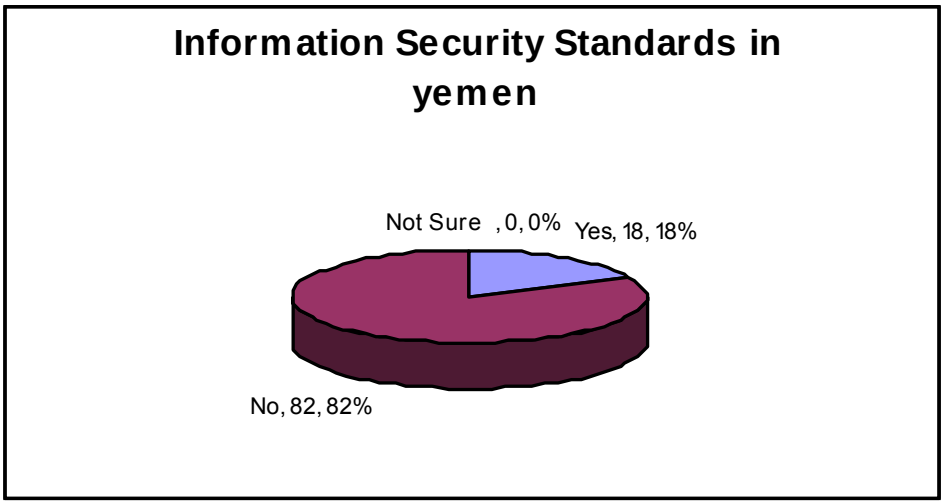

Figure 5-7: The coexistence of information security standards

- **Challenges of applying information security standards**

The results of the survey showed in figure 5-8 identified 5 respondents (29%) stated that it is do not have the budget to do so. (0%) selected the lack of the Standards in non-Arabic are hard to understand, 12 respondents (71%) selected the Shortage of qualified people in information security, (0%) stated that it is International standards are difficult to apply in general, 4 respondents (24%) stated it is Not sure .

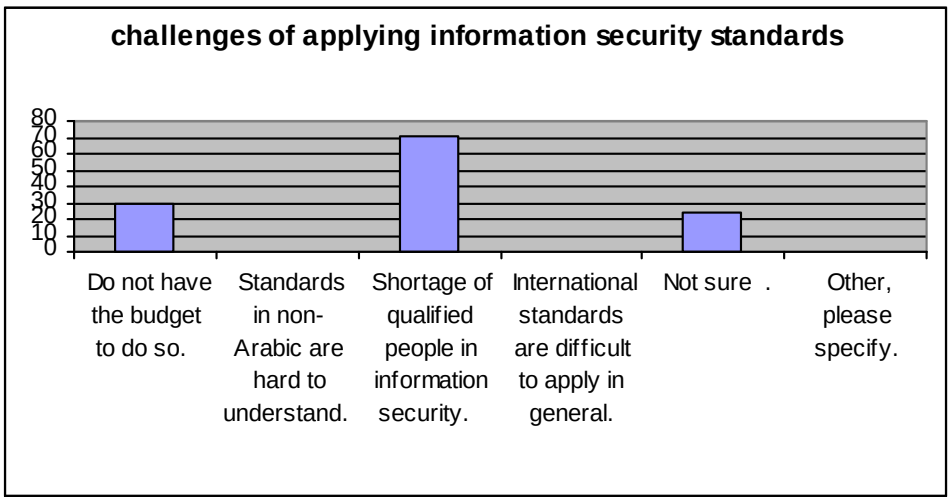

Figure 5-8: the standard Challenges

- **Overcoming these Barriers and Challenges**

The results of the survey showed in figure 5-9 identified 16 respondents (94%) stated that it understands what information security standards are about. (0%) selected the Standards in Arabic language, 5 respondents (29%) selected the Standards created for specific local needs, (0%) stated that it is Special

standards for small and medium enterprises, 15 respondents (88%) stated it is Having employees with training in information security, 11 respondents (65%) selected the Help of a consulting organization in information security..

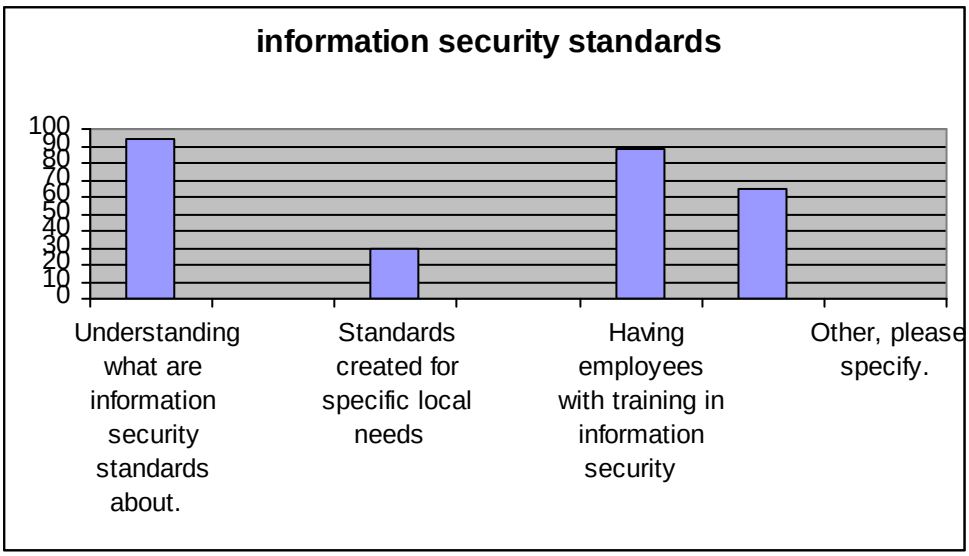

Figure 5-9: Overcoming for standard Challenges

- The results of the survey showed in figure 5-10, a total of 14 respondents (82%) confirmed that they will feeling more secure If he applied information security standards whilst 3 respondents (18%) negated that and (0%) answered with somewhat.

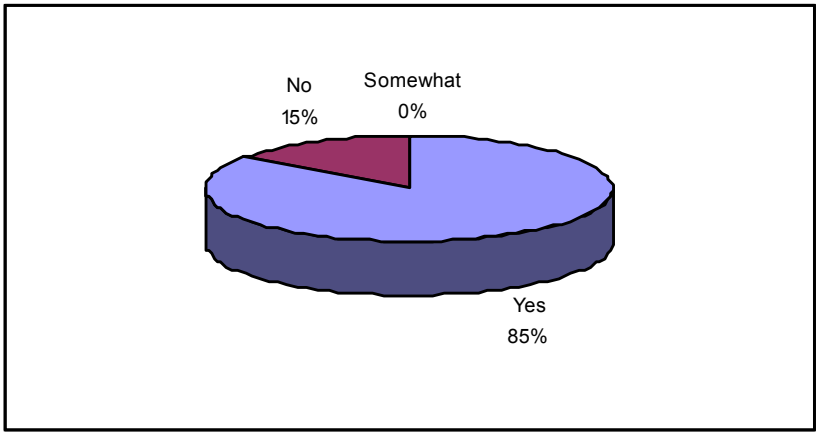

Figure 5-10: feeling secure with security standards

- **Technology challenges:**

The results of the survey showed in figure 5-11 identified 10 respondents (59%) stated that it is due to the lack of competencies related to the technology applied. The 6 respondents (36%) selected the lack of the lack of security policies as the main reason, 14 respondents (82%) selected the lack of in-depth threat analysis done prior to any technology implementation,7 respondents (41%) stated that it is due to the lack of management and monitoring, 4 respondents (24%) stated it is due to decision is always based on commercial aspects not technical/security requirements, 3 respondents (18%) selected the integration with other technologies, and (0%) said it is due to placing the right technology in the wrong place and a single respondent highlighted

that it might be due to other reasons.

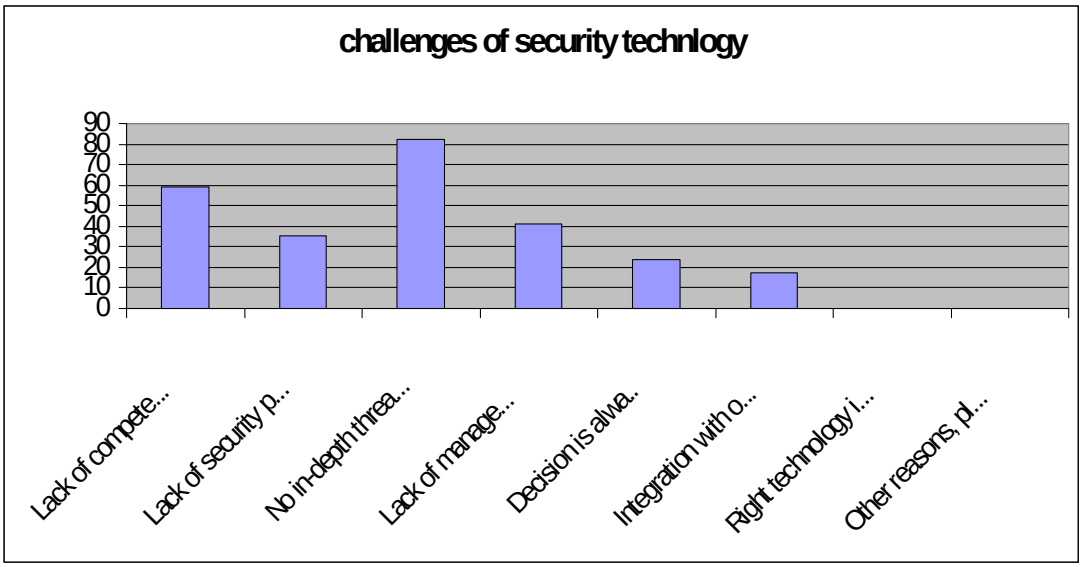

Figure 5-11: Technologies Challenges

- **Challenge an e-government is facing in terms of information flow:**

The results of the survey showed in figure 5-12 identified 16 respondents (94%) stated that the challenges an e- government is facing in terms of information flow are related to the trust between the e- government body and the government departments. The 10 respondents (59%) indicated that it might be due to no common rule and or standard which control this flow of information. Technical challenges were identified by 9 respondents (53%) while 4 respondents (24%) stated that it is due to the absence of direct relation between the government

departments and the e-government except on the services the e-government offers. Only 12 respondents (71%) stated that it is due to no assurance in data classification or declassification.

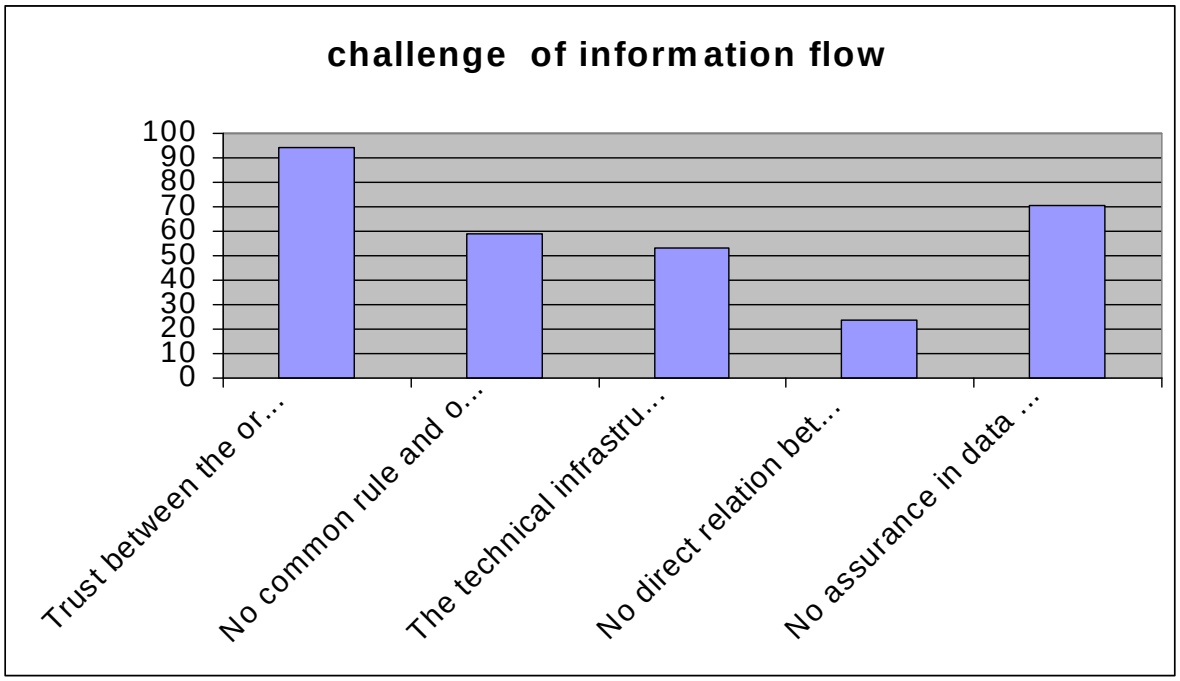

Figure 5-12: information flow Challenges

Question three: What are the security requirements to Develop of Information Security Readiness Indicators for the Implementation of E-government in Yemen?

5.9.3 Security requirements to implement of the Yemen e-government

In this section, the research lists the e-government security

requirement according to multilayer model assessment. The list consists of missing factors to face security risk in future. From table 5-10 that shows the weakness points that are missing factors in the Yemeni government. And these factors are the security requirements to improve security readiness for implement of the e-government of yemen and to facing the security threats and risks. These factors are determent below according to multilayer model layer.

5.9.3.1 Technologies requirements

The Yemen e-government needs these technologies:

- Intrusion Detection and Prevention.
- Files Integrity Checks Software that generates, stores, and compares message digests for files to detect changes to the files.
- Cryptography technique in order to hide their semantic content, prevent their unauthorized use.
- Virtual private network (VPN) to provides a secure communications tunnel for data and other information transmitted between government organization networks.
- Vulnerability Scanning Tools to scanning, description and evaluation of the vulnerabilities in an information system.

- Digital Signatures and Certificates to provide authentication and integrity protection.
- Biometrics to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.
- Security Protocols such as IPSec and SSL to securing Internet Protocol (IP) communications.

5.9.3.2 Policies requirements

The Yemen e-government needs many policies which considered an essential for the Yemen e-government organizations that's to know what they are to do with security issues in regard to assurance high level in security. These are some policies that would be increased due to new need from e-governments or occurrence new threats. These are policies related to the security issues as follow:

- Password Management
- Logs Handling
- Computer Viruses
- Intellectual Property Rights
- Data Privacy
- Privilege Control

- Data Confidentiality
- Data Integrity
- Internet Connectivity
- Administrative Policies
- Encryption Policies
- HR Security Policies
- Third Party Policies
- Physical Security Policies
- Operation Security Policies.

5.9.3.3 Competencies requirements

The Yemeni e-government need some Competencies to increase the staff skills which will assist the government organizations enhancing security and narrow gap of security knowledge among and within the government organizations and keeping mutual trust between citizens and organizations.

The information security competency program should cover the baseline topics of the security knowledge such as:

- Security Operation and management
- Security Architecture and development
- Ethical Hacking

- Security policies and development
- Computer Forensics
- Cryptography
- Security Programming
- Laws and regulations
- Security implementation and configuration
- Security Analysis

5.9.3.4 Operations and Management requirements

The Yemeni e-government needs Management and operational tools in order to enable security practitioner to perform task and achieve the best objectives. There are tools and functions requirement by the Yemeni e-government to accomplish the security monitoring and management:

- Operational Policies and procedures as a rules and regulations where the security Operational staff will follow in performing the tasks expected from them.
- Management Tools.
- Correlation and data mining to ease the process and will allow the operational staff to contribute better in the analysis and response to attacks.

- Reporting and Response
- Analysis and human intervention.

5.9.3.5 Decision requirements

The Yemeni e-government needs Decision making factors which will assist in reaching the decision for selecting or considering a security technology, policy, operational procedure, or hiring a resource with certain security competency. There are factors requirement by the Yemeni e-government to accomplish the Decision making:

- The cost which derives the decision of the security management of the organization.
- The awareness of technologies to select. and
- The availability of these technologies.

5.10 Summary

In this chapter the analysis results showed as follow:

- The current status of the security readiness for implementation of e-government project in Yemen is still weak; it need more time to raise the security readiness indictor. The Yemen government needs many issues to be implemented before

starting the application of e-government project in order to increase trust of citizens, other organizations and to avoid project failure.

- The results showed the security gap between the current situations to security of the information in the government organizations which is (66%) approximately.
- The study showed that (71%) the highest Challenge of applying information security standards identified is the shortage of qualified people in information security, and to overcoming this Challenge are (94%) having employees with training in information security, (88%) Understand what are information security standards about, and (65%) the Help of a consulting organization in information security. The highest Technology challenges identified are (59%) the lack of competencies related to the technology applied, and (82%) the lack of in-depth threat analysis done prior to any technology implementation. And The highest 3 general Challenge an e-government facing in terms of information flow identified are (94%) the trust between the government organizations, (71%) no assurance in data classification or declassification, and

(59%) no common rule and or standard which control this flow of information.

- This chapter presents the second step of achieving the main objective of this study, which concerned with application of the developed mathematical model and questionnaire that provide s-readiness indicators, based on the security factors of the multi-layer model. The study is using the mathematical model for development of security readiness in organizations of the Yemeni government to implementation of e-government. The practical investigation of Yemen includes the evaluation of indictors and weights for 47 measures with the multi-layer model layers, associated with the security readiness indicator. The results of the practical investigations presented in this chapter provide indicators associated with the various layers of the multi-layer model. The indicators provides a comprehensive picture of the strengths and the weaknesses points of information security in organizations of the Yemeni government; and this would help them in their future effort toward future information security readiness improvement and determines the security requirement.

CHAPTER SIX

SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

6.1 Introduction

This chapter includes the research summary, conclusion, the researcher's recommendations for the success of the implementation security readiness, and the researcher’s recommendation for future research.

6.2 Overview of the research study

This research is divided into six chapters.

Chapter one focuses on the introduction of the research as well as background of the research, research problem, research objectives, research questions, significance of the research and related terms and definition of this research. Chapter Two includes literature review related to e-government security, security models, and multi-layer model components and give a view about Yemen’s e-government. Chapter Three covering the research methodological approaches used in the study, which in this case

was mixed methodology. It contains detail description of qualitative and quantitative research designs, sampling plans, data collection instruments, data collection measurements, and data analyzing methods, validity and reliability. Chapter four introduces the mathematical model for multi-layer model for assessment e-government security and describes the method of assessment the security readiness indicators at all layer. Chapter five includes analysis of findings using support graphs, tables, other ways of presenting, and clarifying results. In final, Chapter six includes detailed information about the study, findings & discussion of the findings, and how they relate to the e-government security. It relates the findings to the research objectives, discusses limitations of the study and offer recommendations for future.

6.3 Research Summary

The findings of the research are summarized according to the research objectives as shown below.

- **The first objective is concerned with the "Developing of a mathematical model that provides a new approach for assessment; this approach introduces an analytical method for assessment, which accommodates the various factors considered,**

both individually and collectively, according to the multilayer model layers".

This study supports the use of the mathematical model. The work presented in chapter four from this study presents the steps to make Multi-layer mathematical model which is the first objective of the thesis. It is concerned with the development of a mathematical model that Provides security readiness indicators based on the multi-layer model factors. It gives an integrated view of the model, with illustrations of how to provide indicators, for the evaluation of information security readiness, according to the multi-layer model. It provides useful tools for the assessment information security readiness for e-government. The assessment form associated with the model show how the assessment can be conducted, and how results can be derived and presented.

- **The second objective is associated with "Using of the model for the investigation of information security readiness in Yemen government organizations for implementation of e-government".**

This study presented practical study. The work presented in chapter five presents the second step of the achievement of the main objective of

this study, which is concerned with the application of the developed mathematical model and questionnaire that provide s-readiness indicators, based on the security factors of the multi-layer model. The study is using the mathematical model for the development of security readiness in Yemen government organizations to implementation of e-government. The practical investigation of Yemen e-government included the evaluation of measures and weights for: “47” factors concerned with the multi-layer model layers; “five” layers associated with the s-readiness indicator. The results of the practical investigations presented in chapter five provide indicators associated with the various layers of the multi-layer model. The indicators provide a comprehensive picture of the strengths and the weaknesses of information security in these Yemen government organizations; and this helps them in their future effort toward future information security readiness improvement. And to ensure the validity of the mathematical model Since Yemen was taken as a case study, the model was sent to Yemeni government organizations security managers for verification and Validation. The model was evaluated by the Yemeni government security team and consultants were found to be applicable to the current needs of the government organizations and were imperative as the participants should be part of the e-government initiative. The

validation process was evaluated the mathematical model and its usability. It also included a form for questionnaire, based on the model, for self assessment of s-readiness indicators, by government organizations wishing to enhance their information security.

- **For the sub-objective (a) "Assessing of security readiness for the implementation of e-government in the Yemen's organizations".**

The study showed a set of results including:

Current status of the security readiness for implementation of e-government project in Yemen is still weak; the indictor of security readiness is (0.7) that mean that the government organizations achieved about only (34%) of the multi-layer model requirements. (44%) of security techniques requirements are not applied in government organizations, (77%) of security Operations and Management requirements are not applied in government organizations, (62%) of security policies requirements are not applied in government organizations, (76%) of security Competencies requirements are not applied in government organizations, and (33%) of security decision-making requirements are not applied in government organizations. The study showed that the officials for the security information and decision maker related to information

security in government organizations do not have the efficient management of information security also about (88%) don't have special qualification on IT and information security, (65%) of these selected organizations don't have separate information security department, (82%) of these selected organizations don't applied a security standards, there is no special legal legislation to control electronic transactions, and there is no security strategy for e-government. The study showed that online services are few and limited in some organizations, where about (24%) of these apply Two-Way Interactive e-services and (76%) Information publishing, The results showed the security gap between the current situations to the information security in the government organizations and should be in the situation that around (66%) approximately.

- **For the sub-objective (b) "Identifying the current status of information security and clarifying strengths and weaknesses points, for Yemen's government organizations".**

The study identified main security readiness which states strengths and weaknesses for Yemen's government organizations to implement of the e-government in Chapter five of this study. Table 6-1 gives a list of

missing and existing factors in organizations of the Yemeni government.

Table 6-1: strength and weaknesses factors in organizations of the Yemeni government

layer	Strength points	weaknesses points
Technology	- Access Control. - Anti-Virus & Malicious Code. - Authentication and Passwords. - Logical Access Control (Firewalls).	- Intrusion Detection and Prevention. - Files Integrity Checks. - Cryptography. - VPN. - Vulnerability Scanning Tools. - Digital Signatures and Certificates - Biometrics - Security Protocols
policy	- Log-in Process.	- - Password Management - Logs Handling - Computer Viruses - Intellectual Property Rights - Data Privacy - Privilege Control - Data Confidentiality - Data Integrity - Internet Connectivity - Administrative Policies - Encryption Policies - HR Security Policies - Third Party Policies - Physical Security Policies - Operation Security Policies

COMPETENCIES		- Security Operation and management. - Security Architecture and development - Ethical Hacking - Security policies and development - Computer Forensics - Cryptography - Security Programming - Laws and regulations - Security implementation and configuration - Security Analysis
OPERATIONS AND MANAGEMENT		- Operational Policies and procedures - Management Tools - Correlation and data mining - Reporting and Response - Analysis and human intervention
DECISION	- Need	- Cost - Awareness Technologies Availability

- **For the sub-objective (c) "Identifying the security challenges that influences the Implementation of e-government initiatives in the government of Yemen".**

The study showed that (71%) the highest Challenge of applying information security standards identified is the shortage of qualified people in information security, and to overcoming this Challenge are (94%) having employees with training in information security, (88%) Understand what are information security standards about, and (65%) the

Help of a consulting organization in information security. The highest Technology challenges identified are (59%) the lack of competencies related to the technology applied, and (82%) the lack of in-depth threat analysis done prior to any technology implementation. And The highest 3 general Challenge an e-government facing in terms of information flow identified are (94%) the trust between the government organizations, (71%) no assurance in data classification or declassification, and (59%) no common rule and or standard which control this flow of information.

- **For the sub-objective (d) "Establishing the security requirements for Yemeni's organizations to implement of the e-government".**

This research lists the e-government security requirement in chapter five. These factors are the security requirements to improve security readiness for implement of the e-government of Yemen and to facing the security threats and risks. These factors are determent below according to multilayer model layer.

1. Technologies requirements

The Yemen e-government need there technologies:

- **Intrusion Detection and Prevention.**
- **Files Integrity Checks** Software that generates, stores, and compares message digests for files to detect changes to the files.
- **Cryptography technique** in order to hide their semantic content, prevent their unauthorized use.
- **Virtual private network (VPN)** to provide a secure communications tunnel for data and other information transmitted between government organization networks.
- **Vulnerability Scanning Tools** to scanning, description and evaluation of the vulnerabilities in an information system.
- **Digital Signatures and Certificates** to provide authentication and integrity protection.
- **Biometrics** to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.
- **Security Protocols** such as IPSec and SSL to securing Internet Protocol (IP) communications.

2. Policies requirements

The Yemen e-government needs many policies which considered an essential for the Yemen e-government organizations that's to know what they are to do with security issues in regard to assurance high level in security. These are some policies that would be increased due to new need from e-governments or occurrence new threats. These are policies related to the security issues as follow:

- **Password Management**
- **Logs Handling**
- **Computer Viruses**
- **Intellectual Property Rights**
- **Data Privacy**
- **Privilege Control**
- **Data Confidentiality**
- **Data Integrity**
- **Internet Connectivity**
- **Administrative Policies**
- **Encryption Policies**
- **HR Security Policies**
- **Third Party Policies**

- **Physical Security Policies**
- **Operation Security Policies.**

3. Competencies requirements

The Yemeni e-government need some Competencies to increase the staff skills which will assist the government organizations enhancing security and narrow gap of security knowledge among and within the government organizations and keeping mutual trust between citizens and organizations.

The information security competency program should cover the baseline topics of the security knowledge such as:

- **Security Operation and management**
- **Security Architecture and development**
- **Ethical Hacking**
- **Security policies and development**
- **Computer Forensics**
- **Cryptography**
- **Security Programming**
- **Laws and regulations**
- **Security implementation and configuration**

- **Security Analysis**

4. Operations and Management requirements

The Yemeni e-government needs Management and operational tools in order to enable security practitioner to perform task and achieve the best objectives. There are tools and functions requirement by the Yemeni e-government to accomplish the security monitoring and management:

- **Operational Policies and procedures** as a rules and regulations where the security Operational staff will follow in performing the tasks expected from them.
- **Management Tools.**
- **Correlation and data mining** to ease the process and will allow the operational staff to contribute better in the analysis and response to attacks.
- **Reporting and Response**
- **Analysis and human intervention**.

5. Decision requirements

The Yemeni e-government needs Decision making factors which will assist in reaching the decision for selecting or considering a security

technology, policy, operational procedure, or hiring a resource with certain security competency. There are factors requirement by the Yemeni e-government to accomplish the Decision making:

- The **cost** which derives the decision of the security management of the organization.
- The **awareness** of technologies to select. and
- The **availability** of these technologies.

- **For the sub-objective (e) "provide a security model for Yemen e-government".**

The survey questionnaires focused on importance of factors for organization. The results of the analysis confirmed need all of the factors (sub layers) proposed by the multi-layer model. So , the study suggested the multi-layer model with all elements is a model proposed for the Yemeni government organizations to secure the exchange of information among them and also information security management.

- **For the sub-objective (f) "provide recommendations that can assist the government of Yemen in the implementation of the e-**

government".

The study proved some the recommendations which showed in section (6.4).

6.4 Research Recommendations

In this section the researcher listed some recommendations according to study results. In addition to list some recommendations which were applied in successful projects in developing countries; these recommendations were very important for e-government project in these countries and tend to assist the Yemen's government to implement them to the e-government.

- Increasing of information security indicators by providing security requirements which listed in this thesis.
- Adapting of the multi-layer model as information security standard for the Yemeni organizations with the approach which was given in this thesis.
- Adapting of information security of the national policy.
- Equipping of information security infrastructure in all government organizations.

- Equipping of security training plan for information security staff in all government organizations.
- Equipment of security awareness program for organizations and citizens.
- Coordination with the higher education sector to conduct studies and research in field of information security and e-government security.
- Getting useful experience from the foreign countries in field of information security and to confront hacker's field.
- Coordination and cooperation with the International Telecommunication Union (ITU) to support the Yemen government in field of e-government applications Internet Protocol, and supervision of Internet resources.
- Issuing laws and legislation to combat cyber crimes and information security to confront security threats.
- Training of security officers, investigations, digital forensics, criminal justice, developing IT skills and knowledge to deal with different aspects related to the crimes of information, anti-cyber crime and digital forensics.

- Establishing of a national information security center for Yemeni e-government to identifying security policies , adoption of uniform security standards, propose of the security legislation, and identify training programs for information security staff.
- Establishing a national center for Digital Certification to create infrastructure of public key (PKI) to provide a secure environment that ensure security, confidentiality of electronic transactions, identification of clients, integration of safety, exchange of letters between them, determine the mechanism for issuing digital certificates, and requiring for certification authorities and technical specifications for electronic signatures.

6.5 Research Limitations, Contribution, and Suggestions for Future Research

In this section, the researcher was determent the study Limitations, Contribution, and Suggestions for Future Research.

6.5.1 Limitation of the Study

This study is limited to the government sectors of Yemen country. In addition, this study evaluates the security readiness within there sector in order to exchange or share information with the other organizations only.

6.5.2 Research Contribution

The work has the following contributions for researchers and government

- It provides a new approach for assessment of security readiness indicators, based on a mathematical model according to the multi-layer model.
- This research will help decision makers and employees on the implementation of e-government in Yemen to overcome some of the problems and challenges that await them in the future during implementation.
- This research is a useful source and literature review for the e-government security.
- Finally, The importance of the research, its first study in this field in Yemen.

6.5.3 Suggestions for further research

Although the study had limitations, therefore the research can be done on the following issues:

- Further studies after a period of time and compare the present results of the study, and calculate the gap between them.
- Complete work of a multi-layer model to cover all security aspects of e-services in e-government.
- Further study to measure level of security awareness of the leadership and IT engineers in government organizations, public employees, and citizens of Yemen.
- Further studies to measure security readiness in the private sector, measuring the gap between the private sector and government sector, and getting mutual interests.

REFERENCES

- Al-Azazi, S. (2008). A multi-layer model for e-government information security assessment, Ph.D. thesis, Cranfield University.
- Alavi, M. & Carlson, P. (1992). A Review of MIS Research and Disciplinary Development, Journal of Management Information Systems 8(4), 45-63.
- Alhamdani, W. (2007), Assessment Of Need And Method Of Delivery For Information Security Awareness Program, Proceedings Of The 2006 Information Security Curriculum Development Conference, Infosec CD, 22-23 Sep 2006,Kennesaw, GA, United States, Association For Computing Machinery, New York, NY, 102-109.
- AL-Rabiah, A. (2007), Risk Analysis for the Development of Security-Readiness Indicators for Intranets, Master THISES, Collage of Engineering, King Saud University.
- AL-Rabiah, A. And AL-Bakry,.(2007), A STOPE Model For The Investigation Of Compliance With ISO 17799-2005, Information

Management & Computer Security, King Saud University, 15(4), 283-294.

- AL-Osaimi, K., (2007), Mathematical models for e-readiness assessment of organizations with intranets, Master THISES, Collage of Engineering, King Saud University.
- AL-Osaimi, & Al-heraish And Bakry, (2008), An Integrated STOPE Framework For E-Readiness Assessment, Saudi Computer Journal, 6(2), 23-36.
- Alsohybe.N. (2007), The Implementation Of E-Government In The Republic Of Yemen: An Empirical Evaluation Of The Technical And Organizational Readiness, Ph.D. Thesis, Capella University, US.
- Anderson, R. (2001), Security Engineering: A Guide Building Dependable Distributed Systems, 1st Ed, John Wiley & Sons, Inc, U.S.
- Atreya, M., Hammond, B., Paine, S., Starrett, P. And Wu, S. (2002), Digital Signatures, Mcgraw Hill, New York.
- ARC (2002), Bulgaria: Ict Infrastructure and E-Readiness Assessment, Retrieved From (www.arc.online.bg).

- Awadi, M. (2009), A Study Of Employees' Attitudes Towards Organizational Information Security Policies In The UK And Oman, Ph.D. Thesis, 10-39.
- Baker, W. And Wallace, L. (2007), Is Information Security Under Control? Investigating Quality In Information Security Management", IEEE Security & Privacy, 5(1), 36-45.
- Barnett, F. (1996), Computer Security Training And Education: A Needs Analysis, 6-8 May 1996, Oakland, CA, USA, IEEE Comput. Soc. Press, Los Alamitos, CA, USA, 7- 27.
- Baskerville, R., & Siponen, M. (2002),An Information Security Meta-Policy For Emergent Organizations. Logistics Information Management, 15 (5,6), 337-347.
- BENBASAT, I., GOLDSTEIN, D. & MEAD, M. (1987), The Case Research Strategy In Studies Of Information Systems, MIS Quarterly, 11(3), 369-387.
- Biermann, E., Cloete, E. And Venter, L. (2001), A Comparison Of Intrusion Detection Systems, Computers And Security, 20(8), 676-684.
- Bishop, M. (2005), Introduction To Computer Security, Addison-Wesley.

- Bjorck, F. (2001), Implementing Information Security Management Systems – An Empirical Study Of Critical Success Factors. Lic Thesis. Stockholm University & Royal Institute Of Technology.
- Brewer, D& Nash, M. (1989), Chinese Wall Security Policy, Security And Privacy, 1989 IEEE Symposium, 1-3 May 1989, Oakland, CA, USA, 206-215.
- Brown, S. (2001), Implementation Virtual Private Networks, 1st Ed, McGraw-Hill, New York, USA.
- Bryman,A & Bell,E.(2003), Business Research Models, Oxford University Press New York.
- Bui, X., Sankaran, S. & Sebastian, M. (2003), A framework for measuring national e- readiness, International Journal of Electronic Business, 1(1), 2 - 23.
- Canavan, S. (2003), An Information Security Policy Development Guide For Large Companies, SANS Institute.
- Certification Europe, (2005), International Standards In Information Security, Retrieved From: <Http://Www.Certificationeurope.Com/Services/Info_Security.Asp>
- Coelho,(2007), SECURITY CERTIFICATION FOR ORGANIZATIONS A FRAMEWORK TO MANAGE

INFORMATION SECURITY), stituto Superior de Ciências do Trabalho e da Empresa.

- Cohen, F. (1992), Defence In Depth Against Computer Viruses, Computer And Security, 11(6), 79-564.
- Cole, E. (2002), Hackers Beware-Defending Your Network From Wiley Hacker, 1st Ed, New Rders Publishing, US.
- Cooper, D. & Schindler, P. (2003), Business Research Methods, 8th Ed, Singapore, Mcgraw-Hill.
- Creswell, J. (2003), Research Design: Qualitative, Quantitative, And Mixed Methods Approaches, 2nd Ed ,14-16.
- Creswell,J.(2003), Research Design: Qualitative, Quantitative, And Mixed Methods Approaches 2nd Ed , 35-39.
- Creswell,J. (2003), Research Design: Qualitative, Quantitative, And Mixed Methods Approaches 2nd Ed , 35-39.
- Creswell, J. (1994), Research Design: Qualitative & Quantitative Approaches. Sage Publications Inc.
- Creswell, J. (2003), Research Design: Qualitative, Quantitative, And Mixed Method Approaches, Thousand Oaks, CA,Sage.
- David, J. (2002), Policy Enforcement In The Workplace, Computers & Security, 506-14.

- Dawes, S. S., Bloniarz, P. A. & Kelly, K. L. (1999). Some assembly required: Building a digital government for the 21st century. Report of a Multidisciplinary Workshop Held in October 1998. Retrieved May 5, 2001 from the World Wide Web: http://www.ctg.albany.edu/research/workshop/dgfinalreport.pdf
- Dhillon, G. (1999), Managing And Controlling Computer Misuse. Information Management & Computer Security, 7 (4), 171-176.
- Dhillon, G. (2001), Challenges In Managing Information Security In The New Millennium, In.
- Dhillon, G. (2006), Principles Of Information Systems Security, Text And Cases. New York, John Wiley And Sons.
- Dhillon, G., & Backhouse, J. (1996), Risks In The Use Of Information Technology Within Organizations. International Journal Of Information Management, 16 (1), 65-75.
- Dhillon, G., & Backhouse, J. (2000), Information System Security Management In The New Millennium. Communications Of The ACM, 43 (7), 125-129.
- Doherty, N. F., & Fulford, H. (2005), Do Information Security Policies Reduce Theincidence Of Security Breaches: A Exploratory Analysis. Information Resources Management Journal, 18 (2), 21-40.

- Doughty, K. (2003), "Information Systems Control As Implementing Enterprise 1Cabinet Office, (2002), Security Architecture E-Government Strategy.V2.0, Office Of The Envoy, Retrieved From: <Www.Cabinetoffice.Gov.Uk/Media/252571/Security_Architecture_V2.Pdf >.
- ESCWA, (2009), Reports Of The Regional Profile Of The Information Society In Western Asia, “National Profile Of The Information Society In Yemen “United Nations, New York.
- Fang, Z. (2002), E-Government In Digital Era: Concept, Practice, And Development”, International Journal Of The Computer, The Internet And Management, 10(2), 1-23.
- Gelbsein, E. (2001), Managing Information Security, OECD Workshop, International Computing Centre, Geneva, Retrieved From: Http://Accsubs.Unsystem.Org/Ccaqfbintranet/Productivity/IT/Managing%20information%20security%20OECD.Pdf.
- Graziano, A. & Raulin. M. (1997), Research Methods, A Process Of Inquiry,3rd Ed, New York, Addison Wesley Educational Publisher Inc.3Goguen, J. & Mesequer, J. (1982), Security Policies And Security Models ,Proceedings Of The 1982 Symposium On Security

And Privacy, 26-28 April 1982,Oakland, CA, USA, IEEE, New York, NY, USA, 11-21.

- Hardy, G. (2006), Using IT Governance And COBIT To Deliver Value With IT And Respond To Legal, Regulatory And Compliance Challenges, Information Security Technical Report, Elsevier Science, 55-62.
- Harris, S.(2003), CISSP All-In-One Exam Guide, 2ed., Mcgraw-Hill.
- Higgins, H. (1999), Corporate System Security: Towards An Integrated Management Approach. Information Management And Computer Security, 7(5), 217-223.
- Hone, K., & Eloff, J. (2002), What Makes An Effective Information Security Policy? Network Security, 20 (6), 14-17.
- Humphreys, T. & Plate, A. PD 3002:2002 Guide to BS 7799 Risk Assessment.London, UK: British Standard Institution, 2002.
- Huth, M. (2001), Secure Communicating System-Design, Analysis And Implementation, Cambridge University Press.
- ISACA, (2005) Http://Www.Isaca.Org/Cobit/ (Accessed On 20th October, 2010).
- Jaeger, T. & Rubin, A. (1996), Preserving Integrity In Remote File Location And Retrieval, Proceedings Of Internet Society Symposium

On Network And Distributed Systems Security, 22-23 Feb. 1996, San Diego, CA, USA, IEEE Comput. Soc. Press,Los Alamitos, CA, USA, 53-64.

- Johnson, R. , Onwuegbuzie, A. , & Turner, L. (2007), Toward A Definition Of Mixed Methods Research. Journal Of Mixed Methods Research, 1(2), 112-134.
- Karabacak, B. And Sogukpinar, I. (2005), Information Security Risk Analysis Method , J Comput Secur, 24(147-159).
- Karabacak, B. And Sogukpinar, I. (2006), A Quantitative Method For ISO17799 Gap Analysis, Computer And Security, 25(6), 19-414.
- King, C. , Dalton, C. & Osmanoglu, T. (2001), Security Architecture-Design, Development & Operations, Business And Application Drivers -Case Study, Mcgraw-Hill/Osborne.
- Kraemer, K. & King, J. (2003), Information Technology And Administrative Reform: Will The Time After E-Government Be Different? Retrieved From Http://Crito.Uci.Edu/Publications/Pdf/Egovernment.Pdf,3.
- Kurtz, R. & Vines, R. (2002), CISSP Prep Guide, 1st Ed, Wiley.
- Leedy, P. & Ormrod, J. (2005), Practical Research: Planning And Design. New Jersey, Prentice Hall, 64-85.

- Liska, A. (2003), The Practice Of Network Security,Deployment Strategies For Pro-Duction Environment, Prentice Hall PTR, Pearson Education Inc.
- Liu,(2001),AN E-GOVERNMENT READINESS MODEL, NIVERSITY OF NORTH TEXAS.
- Luker, M. & Petersen, R. (2005), Computer And Network Security In Higher Education,San Francisco, Jossey-Bass.
- Madigan, E. & Petrulich, C., & Motuk, K. (2004), The Cost Of Non-Compliance-When Policies Fail. Proceedings Of The 32nd, Annual ACM SIGUCCS Conference On User Services, 47-52.
- Maxwell, J. (1992), Understanding And Validity In Qualitative Research Harvard Educational Review, 62(3), 279-301.
- Manuel,(2006), Adopting an Information Security Standard for Certification purposes in South Africa, TSHWANE UNIVERSITY OF TECHNOLOGY.
- Mclean, J. (1990), "Security Models And Information Flow, Proceeding.1990 Ieeecomputer Society Symposium On Research In Security And Privacy, 7-9 May 1990,Oakland, CA, USA, 7- 181.
- McClure, S., Scambray, J. And Kurtz, G. (2002), Hacking Exposed Cryptography,Mcgraw-Hill/Osborne.

- Mckosky, R. (1990), File Integrity Checking System To Detect And Recover From Programme Modification Attacks In A Multi-User Computer Systems, Computer & Security, 9(5), 46-432.
- Miles, M. & Huberman, A. (1994), Qualitative Data Analysis: An Expanded Sourcebook,2nd Ed, Thousand Oaks, CA, Sage.
- MCIT, (2005), Ministry Of Telecommunication And Technology, National IT Program :E-Government. Annual Report.
- Mintzberg, H. (1979), An Emerging Strategy Of Direct Research .Administrative Science Quarterly,24,580 -590.
- Moeller, R. (1981), Computer Control And Security, 1st Ed, Wiley, New York.
- MS,Douglas, (2010), Is/It Research: A Research Methodologies Review, Journal Of Theoretical And Applied Information Technology, 4.
- Nachtigal ,S. (2009), E-Business Information Systems Security Design Paradigm And Model, Ph.D. Thesis, 22-30.
- Newman,I.& Benz,R. (1998) Qualitative/Quantitative Research Methodology Exploring The Interactive Continuum,3
- NIC (Yemen National Information Center), (2005), E-Government Between Reality And Expected Goals In Yemen..

- Nijhof, A., Cludts, S., Fisscher, O. & Laan, A. (2003), Measuring The Implementation Of Codes Of Conduct. An Assessment Method Based On A Process Approach Of The Responsible Organisation. Journal Of Business Ethics, 45, 65-79.
- Norris, D. F., Fletcher, P. D., & Holden, S. H. (2001). Is your local government plugged in? Highlights of the 2000 electronic government survey. Working paper, University of Maryland, Baltimore County.
- OECD (2003), The E-Government Imperative, OECD Publications, France.
- ogorman, L. (2003), Comparing Passwords, Tokens, And Biometrics For User Authentication, Proceedings Of The IEEE, 91(12), 40-2022.
- Orlikowski,W & Baroudi, J. (1991), Studing Information Technology In Organization : Research Approaches And Assumption. Information System Research,2(1),1-29.
- Patton, M.& Josang,A.(2004), Technologies For Trust In E-Commerce, Electronic Commerceresearch, 4(1&2),9-22
- Perry, W. (1982), Developing A Computer Security And Control Strategy, 1(1), 17-27.
- Pelitier, T. (1998), Information Security Policies And Procedures,

Auerbach, New York.

- Pfleeger, C. (1997), Security In Computing,2nd Ed, Prentice Hall PTR.
- Pfleeger, C. & Pfleeger, S. (2003), Security In Computing. Prentice Hall, Pearson Education Inc.
- Pinsonneault, A. & Kraemer, K. (1993), Survey Research Methodology In Management Information Systems: An Assessment, Journal Of Management Information SYSTEMS, 10(2), 75-106
- Plexico,K.(2000),Making Privacy The Priority, Federal Computer Weekly, 14(5),47.
- Power, R. (2002), 2002 CSI/FBI Computer Crime And Security Survey, Computer Security Issues And Trends, 8 (1).
- Punch, K. (2003). Survey Research: The Basics. London: Sage.
- Qasem, I. , Yaghi, H. M. And Hubbell, J. (1990), Computer Viruses: Detection And Prevention Techniques, Southeastcon 90 Proceedings, 1, 1-4 April 1990, New Orleans, LA, USA, IEEE, New York, NY, USA, 199-202.
- Rahman, H. (2007), E-Government Readiness: From The Design Table To The Grass Roots, ICEGOV2007, December 10-13, 2007, Macao , China, 230.

- Richardson, R. (2003). CSI/FBI Computer Crime And Security Survey (12), Computer Security Institute.
- Richardson, R. (2007), Computer Crime And Security Survey, 12, CSI.
- Rich, M., & Ginsburg, K. (1999), The Reason And Rhyme Of Qualitative Research:Why, When, And How To Use Qualitative Methods In The Study Of Adolescent Health, Journal Of Adolescent Health, 25, 371-379.
- Risk Advisory Services Group (2006), 2006 Global Information Security Survey;EYG (22), Ernst & Young, UK.
- Robson, C.(2002), Real World Research. 2nded, Malden: Blackwell Publishing.
- Source: UNITED NATIONS GLOBAL E-GOVERNMENT READINESS REPORTS 2008-2010
- Saunders, M. , Lewis, P., & Thornhill, A. (2000), Research Methods For Business Students ,2nd Ed., Prentice Hall.
- Saunders, M. ,Lewis, P. & Thornhill, A. (2003). Research Methods For Business Students, 3nd Ed, Pearson Education Limited.
- Schneier, B. (1996), Applied Cryptography, Protocols, Algorithms And Source Code In C, John Wiley & Sons, Inc, New York

- Schneier, B. (2001), Managed Security Monitoring, Network Security For The 21st Century, Commuter Secur,17(2), 1-13.
- Schneier, B. (2003), Practical Cryptography, 1st Ed, Wiley, US.
- Schneier, B. (2004), Secrets And Lies, Digital Security In A Networked World, 1st Ed, Wiley, US.
- Siponen, M. (2001), Five Dimensions Of Information Security Awareness, Computers And Society, 31(2), 9-24.
- Swanson, R. & Holton, E. (2005),Research In Organizations: Foundations And Methods Of Inquiry, San Francisco,Berrett-Koehler.
- Stake, R. (1995), The Art Of Case Study Research, Thousand Oaks, CA, Sage Publications.
- Tapscott, D. (1995), The Digital Economy: Promise And Peril In The Age Of Networked Intelligence. Mcgraw-Hill.
- Tassabehji,R.(2003), Applying E-Commerce To Business, Sage Publications, New York.
- Tassabehji, R.(2005),Inclusion In E-Government: A Security Perspective, Egovernment Workshop ’ (Egov05), September 13 2005, Brunel University, West London UB8 3PH, UK

- Tassabehji, R.(2005(A)),Information Security Threats. Encyclopedia Of Multimedia Technology And Networking, Pagani, M. Ed, 404-411.
- Tassabehji, R., (2005(B)), Principles For Managing Information Security, Encyclopedia Of Multimedia Technology And Networking, Pagani, M. Ed. 842-849.
- Tayah, A., (2008), Effectiveness of Information Security Management at the Palestinian Information Technology Companies,ms thisis,the Islamic unv., gaza.
- Tiwana, A. (1999), Are Firewalls Enough? Web Security, Digital Press.
- Tipton, H. & Krause, M. (2000), Information Security Management, Auerbach Publications, New York.
- Tomonori, F. & Masanori, O. (2003), Protecting The Integrity Of An Entire File System, Proceedings First IEEE International Workshop On Information Assurance. IWIA 2003, 24 March 2003, Darmstadt, Germany, IEEE Comput. Soc, Los Alamitos,CA, USA, 95-10
- Tryfonas, T., Kiountouzis, E., & Poulymenakou, A. (2001), Embedding Security Practicies In Contemporary Information Systems

Development Approaches. Information Management & Computer Security, 9 (4), 183-198.

- Turban, E., McLean, E., & Wetherbe, J. (1996). Information Technology for Management. New York, NY: John Wiley & Sons, Inc.
- Valentine, N. (2004), E-Government For Developing Countries: Opportunities And Challenges, The Electronic Journal On Information Systems In Developing Countries, 18 (1), 1-25.
- Venter, H. & Ellof, J. (2003), A Taxonomy For Information Security Technologies, Computers And Security, 22(4), 299-308.
- Von, B. &Von, R. (2004), The 10 Deadly Sins Of Information Security Management, Computer And Security, 23(5), 6-372.
- Weirich, D. (2002), Pretty Good Persuasion: A First Step Towards Effective Password Security In The Real World. ACM/SIGSAC New Security Paradigms Workshop, New Mexico.
- Wheeler, P. And Fulp, E. (2007), A Taxonomy Of Parallel Techniques For Intrusion Detection, Proceedings Of The 45th ACM Southeast Conference, ACMSE 2007, Mar 23-Jul 24 2007, Winston-Salem, NC, United States, Association For Computing Machinery, New York, NY 10036-5701, United States, 278-283.

- Wood, C. (2005), Security Policy Made Easy, 10th Ed, Information Shield, U.S.
- Workman, M. (2007). Gaining Access With Social Engineering: An Empirical Study Of The Threat. Information Security Journal, A Global Perspective, 16 (6), 315-332.
- World Bank, (2004), World Bank E-Government, Retrieved From: Http://Www1.Worldbank.Org/ Publicsector/Egov/.
- Yen, D. & Evans, D. (2005), E-Government: Evolving Relationship Of Citizens And Government, Domestics And International Development, Government Information Quarterly.
- Yixin, J., Chuang, L. And Zhangxi, T. (2003), An Authentication Model For Multilevel Security Domains, SMC'03 Conference Proceedings, 2003 IEEE International Conference On Systems, Man And Cybernetics, Conference Theme System Security And Assurance (Cat. No.03CH37483), 5-8 Oct 2003, Washington, DC, USA, IEEE, Piscataway, NJ, USA.
- Yin, R. (2003), C a s e Study Research: Design And Methods, 3rd Ed, Thousand Oaks, Sage.

- Yousafzai,S.& Pallister, J.& Foxall, G.(2005), Strategies For Building And Communicating Trust In Electronic Banking: A Field Experiment. Psychology & Marketing, 22(2),181-203
- Zviran, M. & Haqa, W. (1990), User Authentication By Cognitive Passwords:An Empirical Assessment, Oct 22-25 1990, Jerusalem, Isr, IEEE, Los Alamitos, CA,USA, Pp. P 137-144.
- Zuccato, A. (2004), Holistic Security Requirement Engineering For Electronic Commerce, Computer & Security, 23, 63-77.

Appendices

- Appendix A: **Survey Questionnaires.**
- Appendix B: **List of Ministries- Yemen government organizations.**

Appendix A: **Survey Questionnaires.**

Development mathematical model for
Assessment of information security readiness for implementation of e-government in the Yemen's organizations.

Dear Sir

This survey is associated with a study intended to is concerned with development of Multi-layer mathematical model, and with selecting Yemen government a case-study in order to investigate practical, test validity, increase its usability and assess the information security in Yemen organizations. The assessment is based on the multi-layer model "technology, policy, Operational and management, Competencies, and decision make".

We encourage you to share with us anything you think might be useful in terms of supporting information security efforts in Yemen. Please complete the open-closed questionnaire. Your candid and thoughtful reply will help providing reliable results that can be useful for the future improvement of information security in Yemen organizations in order to assist to implement of e-government project. Please complete the questionnaire by choosing the most correct choice for the issues considered and their corresponding importance. It is estimated that the questionnaire can be completed in approximately sixty minutes. Your feedback is very important to this study, and it would be greatly appreciated if you could take the time to complete the questionnaire your response and comments will be treated with utmost confidentiality. The information collected will not be used to identify individuals or individual organizations, nor will it be publicly disseminated.

Researcher: Jabeir Mohammed Amer

SURVEY QUESTIONNAIRES

Section A: personal Information

1. **Name : (optional**

2. **Age?**

☐ Under25 years ☐ 25-40 years ☐ 41-50 years
☐ 51-60 years ☐ Over 60 years

3. Academic qualifications: degree(s)?

☐ High School-Diploma or less. ☐ Bachelor. ☐ Master.
☐ Doctorate ☐ Other(Specify)

4. Field of study?

☐ Computer Science ☐ Engineering ☐ Management
☐ Business ☐ Other(Specify)

5. Special qualifications in Information Security?

☐ CIW ☐ CISSP
☐ SANS
☐ Other(Specify).

6. Position?

☐ Information Security Manager. ☐ Information Technology Manager
☐ Consultant. ☐ Other (Specify)

7. How long have you been in IS/IT department of your current employer (organization)?

☐ Under 6 Months ☐ 7-12 Months
☐ 13-18 Months
☐ 19-24 Months ☐ Over 25 Months

Section B: Business Information

8. What is the type of your organization?. ☐ Public ☐ Private

9. What is the size of your organization terms of its number of employees?

- Less than 100
- 100 to 500
- 501-1000
- 1001 to 3000
- Over 3000

10. What is the field of your organization?

- Manufacturing
- Banks
- Government
- Oil
- Other (Specify)

11. How long has your organization been in business?

- Under 12 Months
- 13-24 Months
- Over 24 Months

12. Does your organization have separate Information Security Department?

- Yes
- No

13. Number of computers (either PCs or Workstations) in your organization:

- Less than 100
- 100 to 500
- 501-1000
- 1001 to 3000
- Over 3000

14 -What type of e-services your organization is providing?

- Information publishing
- A one way interactive e-service.
- Two-Way Interactive e-services. .
- A transactional e-service.
- A combination of all the above.

Section C: information security factors

This section is a list of information security factors associated with assessment questions, please answer the questions, and give your view of the importance of using the factors for information security. Five levels of importance are given, as explained in the following Table.

1	2	3	4	5
Not at all	Minor	Moderate	Major	Critical

Factors		INDICATOR RESULTS: CURRENT STATE OF FACTOR			IMPORTANCE OF FACTOR				
		Yes	No	Not Sure	MIN				MAX
Security Technologies									
		INDICATOR			IMPORTANCE				
A1	**Do you apply the *Access Control* technology in your organization?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
A2	**Do you use *Intrusion Detection and Prevention* technology?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
A3	**Do you apply the *Anti Virus and Malicious Code* techniques in your organization?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
A4	**Do you apply the *Authentication and Passwords* techniques in your organization?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
A5	**Do you have *Files and Integrity Check* techniques?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

A6	**Do you use *Cryptography* technology?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
A7	**Do you use *VPN* technology?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
A8	**Do you use *Vulnerability Scanning Tools*?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
A9	**Do you apply *the Digital Signatures and Certificates* in your organization?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
A10	**Do you use *Biometrics* technologies ?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
A11	**Do you have *the Logical Access Control (Firewalls)* techniques in your organization?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
A12	**Do you use *Security Protocol (IPsec,SSL,…….)* in your organization?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
	Security Policies								
		INDICATOR			**IMPORTANCE**				
B1	**Do you have in your organization a *policy on* the *Password Management* ?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
B2	**Do you have in your organization a *policy on* the *Log-in Process*?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
B3	**Do you have in your organization a *policy on* the *Logs Handling*?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
B4	**Do you have in your organization a *policy on* the *Computer Viruses*?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
B5	**Do you have in your organization a *policy on* the *Intellectual Property***	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

	***Rights*?**								
B6	**Do you have in your organization a *policy on* the *Data Privacy*?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
B7	**Do you have in your organization a *policy on* the *Privilege Control*?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
B8	**Do you have in your organization a *policy on* the *Data Confidentiality*?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
B9	**Do you have in your organization a *policy on* the *Data Integrity*?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
B10	**Do you have in your organization a *policy on* the *Internet Connectivity*?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
B11	**Do you have in your organization *Administrative Policies*?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
B12	**Do you have in your organization *Encryption Policies*?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
B13	**Do you have in your organization *HR Security Policies*?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
B14	**Do you have in your organization *Third Party Policies*?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
B15	**Do you have in your organization *Physical Security Policies*?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
B16	**Do you have in your organization *Operation Security Policies*?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Security Competencies									
		INDICATOR			**IMPORTANCE**				

C1	**Do you have in your organization competencies in the** *Security Operation and management*?				1	2	3	4	5
C2	**Do you have in your organization competencies in the** *Security Architecture and development*?				1	2	3	4	5
C3	**Do you have in your organization competencies in the** *Ethical Hacking*?				1	2	3	4	5
C4	**Do you have in your organization competencies in the** *Security Policies and development*?				1	2	3	4	5
C5	**Do you have in your organization competencies in the** *Computer Forensics*?				1	2	3	4	5
C6	**Do you have in your organization competencies in the** *Cryptography*?				1	2	3	4	5
C7	**Do you have in your organization competencies in the** *Security Programming*?				1	2	3	4	5
C8	**Do you have in your organization competencies in the** *Laws and regulation*?				1	2	3	4	5
C9	**Do you have in your organization**				1	2	3	4	5

	competencies in the *Security Implementation and Configuration***?**								
C10	**Do you have in your organization competencies in the a** *policy on Security Analysis***?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Security Operations and Management									
		INDICATOR			**IMPORTANCE**				
D1	**Do you use** *Operational Policies and Procedures* **during the administration of information security in your organization ?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
D2	**Do you use Management** *Tools* **during the administration of information security in your organization?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
D3	**Do you make** *Correlation of data collected from all security devices* **during the administration of information security in your organization?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
D4	**Do you make *Reporting*** *and Response* **to incidents in a short time during the administration of information security in your organization?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
D5	**Do you apply** *Analysis for incidents* **during the administration of**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

	information security in your organization?								
Security Decision Factors									
		INDICATOR			**IMPORTANCE**				
E1	**Is the decision-making by providing the needs of information security in your organization based on the *cost*?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
E2	**Is the decision-making by providing the needs of information security in your organization based on the *Awareness*?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
E3	**Is the decision-making by providing the needs of information security in your organization based on the *Need* ?**	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
E4	**Is the decision-making by providing the needs of information security in your organization based on the *Technologies Availability ?***	☐	☐	☐	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

LAYER	IMPORTANCE OF LAYER				
Technology	min				max
	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Policies	min				max
	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Competencies	min				max
	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Operations and Management	min				max
	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Decision Factors	min				max
	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Section D: Information Security Standards and challenges

1. **Does your organization apply any information security standards?**

   ☐ Yes
   ☐ No
   ☐ Not Sure

2. **If your organization applies information security standards, please give the name:**

3. **What do you think are the challenges of applying information security standards in your organization? (Select all that apply)**

   ☐ Do not have the budget to do so.
   ☐ Standards in non-Arabic are hard to understand.
   ☐ Shortage of qualified people in information security.

- [ ] International standards are difficult to apply in general.
- [ ] Not sure .
- [ ] Other, please specify.

4. **What do you think can help your organization in applying information security standards** (**check all that apply**)?

- [ ] Understanding what are information security standards about.
- [ ] Standards in Arabic language
- [ ] Standards created for specific local needs
- [ ] Special standards for small and medium enterprises
- [ ] Having employees with training in information security
- [ ] Help of a consulting organization in information security
- [ ] Other, please specify.

5. **If your organization has already applied information security standards, do you feel more secure in your organization**?

- [ ] Yes
- [ ] No
- [ ] Somewhat

6. **Please select from the list below some of the challenges related to the technologies mentioned on any security technology that can be used in your organization.**

- [ ] Lack of competencies related to the technology

- ☐ Lack of security policies
- ☐ No in-depth threat analysis done prior of implementation
- ☐ Lack of management and monitoring
- ☐ Decision is always based on commercial aspects not technical/security requirements.
- ☐ Integration with other technologies
- ☐ Right technology in wrong place
- ☐ Other reasons, please specify.

7. Select the challenge an e-service /e-government is facing in terms of information flow:

- ☐ Trust between the organizations /governmental organizations.
- ☐ No common rule and or standard which controls this flow of information
- ☐ The technical infrastructure challenges
- ☐ No direct relation between the organizations /government organizations and the e-government except on the services the e-government offers.
- ☐ No assurance in data classification or declassification.

Please give your views on the mathematical model and questionnaire

Other *(Free)* Comments / Suggestions:

Thank you very much…

Appendix B: **List of Ministries - Yemen government organizations.**

- **Ministry of Communication and Information Technology.**
- **Ministry of Finance.**
- **Ministry of Oil and Manorial.**
- **Ministry of Defiance.**
- **Ministry of Interior.**