Islamic University of Gaza

Deanery of Graduate Studies

Faculty of Commerce

Department of Business Administration

Information Security Management for Strategic and Effective Implementation of e-Management in the Governmental Institutions in Gaza

By

Alaa Al-Deen A. Mohammed Hassan

Supervisor

Prof. Majed M. El-Farra

This Thesis is Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Business Administration

Jan, 2013

الجامعة الإسلامية – غزة
عمادة الدراسات العليا
كلية التجارة
قسم إدارة الأعمال

إدارة أمن المعلومات كمدخل استراتيجي لفاعلية تطبيق الإدارة الإلكترونية في المؤسسات الحكومية العاملة في قطاع غزة

إعداد
الباحث: علاء الدين عوض صابر محمدحسن

إشراف
أ.د. ماجد محمد الفرا

قدم هذا البحث استكمالاً لمتطلبات الحصول على درجة الماجستير في إدارة الأعمال

1434هـ - 2013 م

بسم الله الرحمن الرحيم

الجامعة الإسلامية – غزة
The Islamic University - Gaza

عمادة الدراسات العليا

هاتف داخلي: 1150

الرقم.....ج.س.غ/35/..... Ref

التاريخ.....2012/01/21..... Date

نتيجة الحكم على أطروحة ماجستير

بناءً على موافقة عمادة الدراسات العليا بالجامعة الإسلامية بغزة على تشكيل لجنة الحكم على أطروحة الباحث/ **علاء الدين عوض صابر محمد حسن** لنيل درجة الماجستير في **كلية *التجارة*/ قسم إدارة الأعمال** وموضوعها:

إدارة أمن المعلومات كمدخل استراتيجي لفاعلية تطبيق الإدارة الإلكترونية في المؤسسات الحكومية العاملة في قطاع غزة

وبعد المناقشة العلنية التي تمت اليوم الاثنين 09 ربيع أول 1434 هـ، الموافق 2013/01/21م الساعة الحادية عشرة صباحًا بمبنى القدس، اجتمعت لجنة الحكم على الأطروحة والمكونة من:

أ.د. ماجد محمّد الفرّا	مشرفاً ورئيساً	.....
أ.د. يوسف حسين عاشور	مناقشاً داخلياً	.....
أ.د. سامي سليم أبو ناصر	مناقشاً خارجيًا	.....

وبعد المداولة أوصت اللجنة بمنح الباحث درجة الماجستير في **كلية *التجارة*/ قسم إدارة الأعمال**.

واللجنة إذ تمنحه هذه الدرجة فإنها توصيه بتقوى الله ولزوم طاعته وأن يسخر علمه في خدمة دينه ووطنه.

والله ولي التوفيق ،،،

عميد الدراسات العليا

أ.د. فؤاد علي العاجز

P.O. Box 108, Rimal, Gaza, Palestine fax: +970 (8) 286 0800 فاكس Tel: +970 (8) 286 0700 ص.ب. 108 الرمال، غزة، فلسطين هاتف
public@iugaza.edu.ps www.iugaza.edu.ps

Abstract

This study aims to identify the impact of information security management on the effectiveness of applying e-management in the Governmental Organizations in Gaza. The research used the analytical descriptive approach and the comprehensive survey to collect the study data in order to meet research objectives using the Statistical Package for the Social Sciences (SPSS). (158) questionnaires were distributed as a tool to explore the opinions of the study population, the collected questionnaires were (144), represent response rate (91.14%). Ten fields of information security management were investigated at (8) Governmental Organizations along with the effectiveness of applying e-management. The ten fields of information security management include: Security Policy, Organizational Security, Assets Classification and Control, Personnel Security, Physical and Environmental Security, Computer and Network Management, System Access Control, System Development and Maintenance, Business Continuity Planning, Compliance to Legal Requirements.

The study concluded several findings, mainly:

- The effectiveness rate of information security management in the Governmental Organizations in Gaza was (65.30%). Clear weaknesses were found in some fields include: "*Personnel Security*", "*Organizational Security*", "*Compliance to Legal Requirements*" and "*Asset Classification and Control*".
- The effectiveness rate of applying e-management in the Governmental Organizations in Gaza was (74.5%).

The study concluded several recommendations, mainly:

- Government is advised to exert more efforts towards the weak information security fields like: *Personnel Security*", "*Organizational Security*", "*Compliance to Legal Requirements*" and "*Asset Classification and Control*".

ملخص الدراسة

هدفت هذه الدراسة إلى التعرف على أثر إدارة أمن المعلومات على فعالية تطبيق الإدارة الالكترونية في المؤسسات الحكومية العاملة في قطاع غزة، ولإجراء هذه الدراسة تم استخدام المنهج الوصفي التحليلي الذي يعتمد على جمع البيانات عن الظاهرة وتفسيرها، والمسح الشامل لمجتمع الدراسة من أجل تحقيق الأهداف من خلال استخدام برنامج التحليل الإحصائي (SPSS) في تحليل البيانات.

تم توزيع (158) استبانة كأداة رئيسة لاستعراض آراء مجتمع الدراسة، وتم استرجاع (144) استبانة، بمعدل استجابة (91.14%). تمت دراسة (10) مجالات لإدارة أمن المعلومات في (8) مؤسسات حكومية بالإضافة إلى مجال فعالية تطبيق الإدارة الالكترونية. تتكون هذه المجالات العشرة من: سياسة الأمن، والأمن التنظيمي، وضبط الأصول وتصنيفها، والأفراد وأمن المعلومات، والأمن المكاني، وإدارة الشبكة والحواسيب، وضبط الوصول للأنظمة، وتطوير وصيانة الأنظمة، وتخطيط استمرارية العمل، والامتثال للمتطلبات القانونية.

خلصت الدراسة إلى العديد من النتائج وأهمها:

- مستوى فاعلية إدارة أمن المعلومات في المؤسسات الحكومية العامة في قطاع غزة كان (65.3%)، كما أنه يوجد ضعف واضح في بعض المجالات مثل: الأفراد وأمن المعلومات، والأمن التنظيمي، والامتثال للمتطلبات القانونية، وتصنيف الأصول وضبطها.
- مستوى فاعلية تطبيق الإدارة الالكترونية في المؤسسات الحكومية العاملة في قطاع غزة كان (74.5%).

خلصت الدراسة إلى مجموعة من التوصيات وأهمها:

- توصية إلى الحكومة الفلسطينية ببذل المزيد من الجهود لتعزيز مجالات أمن المعلومات وبصفة خاصة المجالات التي بها ضعف واضح مثل: الأفراد وأمن المعلومات، والأمن التنظيمي، والامتثال للمتطلبات القانونية، وتصنيف الأصول وضبطها.

DEDICATION

I would like to take this opportunity to express my deepest thanks and lovingly dedicate this work to:

My dear parents, father-in-law and mother-in-law who have been my constant source of inspiration. They have given me the drive and discipline to tackle any task with enthusiasm and determination,

Dear wife for her understanding, patience and continues support. Without her love and support this research would not have been made possible,

My sons, Ayham and Osama,

Brothers and Sisters,

All my lovely people that I know.

ACKNOWLEDGMENTS

Praise be to Allah, Lord of the Worlds, and prayers and peace on the prophet Muhammad peace be upon him.

This work provides an opportunity for me to express my profound thanks to those people who have submitted to me the aid and assistance for the completion of this work, also to thank those who support me via valuable advises.

I take this opportunity to express my profound gratitude and deep regards to my supervisor Prof. Majed M. El-Farra for his exemplary guidance, monitoring and constant encouragement throughout the course of this thesis. The blessing, help and guidance given by him time to time shall carry me a long way in the journey of life on which I am about to embark.

I also take this opportunity to express a deep sense of gratitude to the examiners of this research; Prof. Yousif H. Ashour and Prof. Samy S. Abu Naser, for their cordial support, valuable information and guidance, which helped me in completing this task through various stages.

I am obliged to staff members of the Governmental Institutions in Gaza, for the valuable information provided by them in their respective fields. I am grateful for their cooperation during the period of my assignment.

Lastly, I thank almighty, my parents, father-in-law, mother-in-law, wife, sons, brothers, sisters and friends for their constant encouragement without which this assignment would not be possible.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BS	British Standard
BSI	British Standards Institution
CIA	confidentiality, integrity and availability
CSFs	cost effective and sustainable frameworks
DMAIC	define, measure, analyze, improve, and control
DSA	digital signature algorithms
DTI	Department of Trade and Industry
GRC	governance, risk management and compliance
IEC	International Electro technical Commission
ISD	information system development
ISMS	information security management system
ISO	International Organization for Standardization
ISRM	information security risk management
JTC1	Joint Technical Committee 1
PDCA	Plan-Do-Check-Act model
PIN	personal identifier number
RSA	RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman
SDPSS	software development process for secured systems
SMEs	small and medium-sized enterprises
SRE	Security Requirements Exercise
STOPE	strategy, technology, organization, people, and environment
UML	unified modeling language
URL	Uniform Resource Locator
W3C	World Wide Web Consortium
WS	web services
XML	Extensible Markup Language

CHAPTER (1)
BACKGROUND CONTEXT

1.1 Introduction

1.2 Research Problem

1.3 Research Hypothesis

1.4 Research Variables

1.5 Research Objectives

1.6 Research Importance

1.7 Previous Studies

1.7.1 Arabic Studies

1.7.2 Foreign Studies

1.8 Comments on Previous Studies

1.1 Introduction

Work environments continue to change with increasing dependence on information technology and the spreading use of internet and the various computer networks. This increasing change leads to the fact that, information systems are subjected to various security threats. Many surveys have indicated that, challenges related to information security are far to be resolved, according to many factors affect the organization success to achieve the needed level to secure its information resources. One important factor is the human challenge represented in the way the working human at an organization deals with his required role that he should commit, and how the organization defines its resources and addresses the surrounded challenges (Ashenden, 2008).

The information technology has become an important part of the modern life, as the use of information technology these days is related to all business sections. Most organizations need information systems to survive and prosper. Consequently, these organizations need to be serious about securing their information assets. Hence, many important operations emerge to protect information assets, that is on a large extent depends on the cooperative human behavior (Rhee, Ryn, & Kim, 2012).

Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the greatest threat to information security. It has become widely accepted that the establishment of an organizational sub-culture of information security is key to managing the human factors involved in information security. Studies in information security consistently report that a lack of the manager and user awareness is the number one obstacle to achieving a good information security posture. Information security refers to the preservation of confidentiality, integrity, and availability of information and the systems that use, store, and transmit information. Awareness of information security is the vigilance in understanding various information security threats and in perceiving vulnerability related to these threats. However, an understanding of threats alone seems insufficient to motivate one to take actual actions (Niekerk & Solms, 2010).

Information security has become very important in most organizations. The main reason for this is that, the access to information and the associated resources has become

easier because of the developments in distributed processing, for example: internet and the electronic commerce. The result is that organizations need to ensure that their information is properly protected and that they maintain a high level of information security. In many cases, organizations demand some proof of adequate information security from business partners before electronic commerce can commence (Solms R. v., 1998a).

Information security has become very important in most organizations. An acceptable level of information security can only be introduced and maintained if the correct set of security controls, both procedural and technical, is identified, implemented and maintained. The process of identifying the most effective set of security controls can be a very complicated, resource-intensive process. A number of large British companies have joined forces to establish a Code of Practice for Information Security Management. This document provides guidelines to any organization to identify and introduce a set of controls that will provide an acceptable level of protection to information resources. The Code of Practice is based on ten categories that should be presented in most organizations, these are: security policy, organizational security, assets classification and control, personnel security, physical and environmental security, computer and network management, system access control, system development and maintenance, business continuity planning, compliance to legal requirements (Solms R. , 1998b).

1.2 Research Problem

In some cases, organizations may fail in achieving the required level of protecting their information resources because of their failure in implementing successful comprehensive plans to manage their information security. There are essential aspects, which, if not taken into account in an information security governance plan, will surely cause the plan to fail, or at least, cause serious flaws in the plan. These aspects can be used as a checklist by management to ensure that a comprehensive plan has been defined and introduced. Because of the importance of these aspects, they will be involved in this study (Solms & Solms, 2004).

This study tries to disclosure the serious flaws in information security management systems in the Government in Gaza, to define its fields and to study its impact on the effectiveness implementation of e-management in the Governmental institutions in Gaza. Also, it will search in the features of applying e-management and the main obstacles that limit its evolvement. On the other side, this study tries to recognize the position of information security management in the Government strategies and to define the level of its commitment and compliance with international standards in the field of information security management.

The research problem could be identified as "**To what extent the information security management is effective in the Governmental institutions in Gaza and what is its impact on the effectiveness of applying e-management there**".

1.3 Research Hypothesis

a. There is a significant statistical correlation at level ($\alpha = 0.05$) between the fields of information security management (security policy, organizational security, assets classification and control, personnel security, physical and environmental security, computer and network management, system access control, system development and maintenance, business continuity planning and compliance to legal requirements) and the effectiveness of applying e-management in the Governmental Institutions in Gaza.

b. There are no significant statistical differences at level ($\alpha = 0.05$) among the respondents in their opinions about the impact of information security management on the effectiveness of applying e-management in the Governmental Institutions in Gaza attributed to their characteristic factors like (gender, qualification, specialty, age, job title, experience and the governmental institution they belong to).

1.4 Research Variables

1.4.1 Dependent Variable

The dependent variable is the effectiveness level of applying e-management in the Governmental institutions in Gaza.

1.4.2 Independent Variables

The independent variables are the fields of information security management, which are:

i. Security Policy.
ii. Organizational Security.
iii. Asset Classification and Control.
iv. Personnel Security.
v. Physical and Environmental Security.
vi. Computer and Network Management.
vii. System Access Control.
viii. Systems Development and Maintenance.
ix. Business Continuity Planning.
x. Compliance to Legal Requirements.

1.5 Research Objectives

Research objectives can be summarized in the following points:

- To recognize the requirements of the effective information security management in the Governmental institutions in Gaza.
- To study the most important dimensions of information security management.
- To evaluate the impact of information security management on the effectiveness of applying e-management in Governmental institutions in Gaza.
- To define the priorities should be addressed by the Government with regard to information security management.
- To understand the correlations between information security management fields and the effective implementation of e-management.

- To obtain essential conclusions and recommendations that should enhance the involvement of information security management in the Government strategies and to enhance the effectiveness level of applying e-management.

1.6 Research Importance

The importance of this study stems from the following aspects:

- This study is considered the first one in this field that has studied the information security management in Governmental institutions in Gaza and its impact on the effective implementation of e-management.
- The utilization of study conclusions and recommendations to identify the priorities and to recognize the gap between the real situation and the prospects in the field of information security management.
- Motivate the researchers' interest to penetrate the fields of information security management and e-management and the requirements to apply each one and the relations between them.

1.7 Previous Studies

1.7.1 Arabic Studies

(Al-Ajez, 2011)

The research paper titled "The role of organizational culture to activate the application of e- management" aimed to identify the role of organizational culture to activate the application of e- management in Ministry of Education and Higher Education – Gaza's Governorates. The researcher used the descriptive analytical method, and distributed a questionnaire to (294) employees dealing with the e-management. The study concluded numbers of results, the most important are: 1) There are significant statistical relationship between the elements of an organizational cultural as (organizational values, organizational beliefs, organizational norms, and organizational expectations) and the activation of the application of e-Management. It was a positive correlation relationship. 2) Not allowed to employee for accomplishing the work of a particular business decisions without returning to his immediate supervisor within the work e-management. 3) Do not

honored or motivate staff for excellence in structuring and dissemination of e-management in the ministry. 4) Not allowed to staff to participate in the development of systems and mechanisms of e-management program they use. The study's recommendations: 1) Encourage staff to express their opinions in the values, beliefs, norms, and expectations established within the Ministry to develop them to suit the environment of e-management, and continuously circulated electronically in terms reflect the ministry culture. 2) Support the Observational learning in order to promote best of e-management practices among staff.

(Al-Aloul, 2011)

The research study titled "The available requirements for successful implementation of e-management at charitable associations in Gaza" aimed to identify the availability requirements for the successful application of e-management in the largest hundred charitable associations operating in the Gaza Strip. The study also aims to recognize the impact of such requirements on the readiness of institutions against corruption. The researcher used the analytical descriptive approach, prepared a questionnaire as a key research tool, distributing it to the executive managers of the largest one hundred charitable associations with 100% recover rate of. Moreover, the researcher conducted four interviews to interpret certain findings. The study concluded several findings, mainly: 1) The availability rate of requirements for the successful application of e-management in the largest charitable associations in Gaza Strip reached 68.92%. 2) The largest charitable associations in the Gaza Strip have an institutional readiness against corruption estimated by 76.68%. 3) There is a direct, significant statistical relationship at the level of significance of $\alpha \leq 0.05$, between the availability requirements for the successful application of e-management in the largest one hundred charitable associations operating in the Gaza Strip and the institutional readiness against corruption. However, some requirements, including organizational, financial, maintenance, information security and soft technical structure, are considered most influential on the institutional readiness against corruption and constitute 56.4% of the total influence. The study has several recommendations, mainly: The need to; sufficiently include the application of e-management within the strategic and operational plans of

associations, focus on the participation of all stakeholders, motivate and train staff to achieve the successful application, develop the technical infrastructure, fortifying it with licensed integrated programs of information security, gradually enhance the websites of charitable associations to interact with the public and render the services, and publish regulations as well as administrative and financial reports.

(Saleh & Alfantookh, 2011)

This paper titled "A new comprehensive framework for enterprise information security risk management (ISRM)" is concerned with presenting a comprehensive ISRM framework that enables the effective establishment of the target safe environment. The framework has two structural dimensions; and two procedural dimensions. The structural dimensions include: ISRM ''scope'' and ISRM ''assessment criteria'', while the procedural dimensions include: ISRM ''process'' and ISRM ''assessment tools''. The framework uses the comprehensive STOPE (strategy, technology, organization, people, and environment) view for the ISRM scope; while its assessment criteria is considered to be open to various standards. For the procedural dimensions, the framework uses the widely known six-sigma DMAIC (define, measure, analyze, improve, and control) cycle for the ISRM process; and it considers the use of various assessment tools. The framework respond to the need of using a ''management criteria'', and permits various criterion to be taken into account, including International Organization for Standardization (ISO) information security controls, and considering pre-determined benchmarks.

(Al-Otaibi, 2010)

This study titled "The information security of websites and its compatibility with local and international standards" aims to identify how information security of websites in security and civil authorities is compatible with the local and international standards whereas the study is looking to answer the following main question: what is the computability extent of the information security of websites in security and civil authorities in Riyadh city to the local and international standards? This study was applied on all of websites staff working at: National Guard, Ministry of Defense & Aviation,

Ministry of Interior, Ministry of Communications and Information Technology, Divan of Grievances and Ministry of Economic & Planning in Riyadh city. The total number of the sample was (254) persons. The random sample number was (195) persons, (111) amongst them are from security authorities, and (84) are from civil authorities. The main study results are: (1) Compatibility degree of the (Information security' strategies) and (Organizing the information security) in websites of both sectors civil and security ones with the local and international standards (Medium). (2) Compatibility degree of the (Information security technologies) and (Information security for people) in websites of both sectors civil and security ones with the local and international standards (High).

(Al-Somairy, 2009)

The research study titled "Availability requirements of the application of electronic management on secondary schools in Gaza Governorates, and development methods" aimed to identify the availability requirements of the application of e-management on secondary schools in Gaza, from the point of view of secondary schools principals, and developing methods. To achieve the aim of the study the researcher followed the descriptive method, and designed questionnaire which is composed of (48) items, distributed on (5) domains: (physical requirements, professional human requirements, management requirements, financial requirements, requirements for safety and security), as well as an opened question at the end, about ways to develop these requirements. The veracity of the questionnaire has been confirmed in two ways: the sincerity of arbitrators and the sincerity of internal consistency, and stability have been confirmed in two ways: the retail way and mid-term alpha Kronbach way. Questionnaire was distributed on a study sample consisting of (124) principals of the secondary schools in Gaza for the academic year (2009/2008). After analyzing the data statistically, the study found that the availability requirements of the application of e-management on secondary schools in Gaza, from the point of view of secondary schools principals are few in general, where the percentage of responding on a resolution in general (50.27%). The study suggested ways to develop the requirements for the application of e-management, depending on analysis of the results, opinions and proposals of the study sample and the results of previous studies.

(Ammar, 2009)

The research study titled "The possibility to apply electronic management in the United Nations Relief and Work Agency – Gaza Field Office" aimed to determine the possibility to apply e-management in the United Nations Relief and Work Agency – Gaza Field Office, through the availability of the necessary requirements for successful application of e-management, such as financial requirements, technical requirements, human resources requirements and the commitment and support of top management, in addition it also aimed to determine the role of using e-management in the improvement of employees performance in the agency. Questionnaire was distributed on a study sample consisting of (225). The study revealed that agency employees aware of e-management and its requirements for successful implementation, necessary requirements needed for the implementation of e-management are available in the agency, the study showed the presence of commitment and support from top management to the implementation of e-management and it always keen to keep abreast of technical developments and to prepare its staff psychologically and morally for the use of e-management, the study also showed individuals support for e-management applications in terms of security and showed that the use of e-management results in increasing significantly the effectiveness and efficiency of job performance due to quick completion of work, raising productivity, quick and accurate delivery of instructions and saving staff time and effort, however the study showed a weakness in the incentives system for outstanding employees in the electronic work and showed that there is a lack of sharing from all administrative levels in setting the goals and programs related to the application of e-management.

(Zoarob, 2009)

The research study titled "The automation role in improving the performance of personnel affairs administration at the governmental ministries in Gaza" aimed to identify automation and its role in improving the performance of personnel affairs administrations in the governmental ministries in Gaza strip. The researcher attempted the descriptive analytical approach through all-inclusive survey of managers and their vices and head of departments who perform the different missions and tasks of the personnel affairs in the governmental ministries. Study results indicated the following: 1) The degree of

implementing or using automation factors is generally acceptable in the governmental ministries. 2) Automation helps effectively in planning, selecting, evaluating and identifying the training needs for the human resources in the governmental ministries. 3) The factors of automation implementation will increase automation effectiveness of personnel affairs administrations. The study suggested the following recommendations: 1) Automation should be relied on during the planning process, as well as in selecting and evaluating the human resources in the governmental ministries. 2) Automation should be relied on when identifying the training needs for the human resources in the governmental ministries. 3) Overcoming the impediments that may face the spreading use of automation through the technical training and viewing proper plans for that.

(Tayeh, 2008)

This study titled "Effectiveness of Information Security Management at the Palestinian Information Technology Companies" aimed to identify the extent of the effectiveness of Information Security Management in Palestinian Information Technology companies (Jerusalem, West bank, and Gaza). The researcher investigated ten domains of information security management in forty one companies. The ten domains included the Information Security Policy, Organizational Security, Asset Classification and Control, Personnel Security, Physical and Environmental Security, Computer and Network Management, System Access Control, Systems Development and Maintenance, Business Continuity Planning, and Compliance. In addition, the researcher studied the differences between the companies in applying Information Security Management due to Company history in Information Technology (IT) field, Operating systems, Staff Qualifications, Staff Experience Years, Company Main Working Field, and Yearly Security Budget. The findings of the research showed that all domains except the Organizational Security were affecting the effectiveness of Information Security Management in Palestinian Information Technology companies. Moreover, there are no differences between the information technology companies in applying the information security management due to the Company history in IT field, Operating systems, Staff Qualifications, Staff Experience Years, Company Main Working Field, and Yearly Security Budget.

(Al-Ghoty, 2006)

The research study titled "The requirements for successful implementation of e-Government at the Palestinian ministries" aimed to investigate the availability of requirements for successful implementation of e-Government in Palestinian ministries, as the clarity of the concept for the senior management, the realization of the advantages of application, the availability of skilled human resources, availability of infrastructure, availability of appropriate awareness to the public, availability of flexible organizational structures, and availability of a simple procedure for work. The researcher used descriptive analytical method, and developed a questionnaire for the purpose of search, which was distributed on (100) employees in seven senior management sites in each ministry of the Palestinian Authority ministries and numbering (22) Ministry, The researcher reached several conclusions, including: the presence of an effective leadership for e-government by 64.7%, and the availability of human requirements by 70.1%, and the availability of technical requirements by 64.5%, and the availability of simpler procedures in Palestinian ministries increased by 67.9%, the study also found that the application of e-government in Palestine will reduce corruption and cronyism by 74%. Eventually, the study concluded several recommendations, including: the senior management in the Palestinian ministries should participate in planning for e-government, and human resources development, and interest in legislation and legal regulations to get legal legitimacy.

1.7.2 Foreign Studies

(Wangwe, Eloff, & Venter, 2012)

This paper "A sustainable information security framework for e-Government – Case of TANZANIA", presented that the government of Tanzania adopted an e-Government strategy in 2009 that is aimed at improving efficiency in the government and providing better services to citizens. Information security is identified as one of the requirements for the successful e-Government implementation although the government has not adopted any standards or issued guidelines to government agencies with regards to information security. Comprehensive addressing of information security can be an

expensive undertaking and without guidelines information security implementations may be more prone to failure. In a resource poor country such as Tanzania, there is a need for a cost effective and sustainable means of addressing information security in e-Government implementations. In this paper the authors present a case study of an e-Government interaction between a ministry and a government agency and the information security challenges identified in the implementation. In order to address these challenges an information security framework is conceptualized using action research. The framework is applied in the case study to address the identified challenges and the means to address future challenges in a sustainable manner is identified. Finally, the proposed framework is evaluated against Tanzanian and international metrics. The framework has been successfully applied to a case study. The evaluation of the framework shows that Tanzania's Government addresses all the cost effective and sustainable frameworks (CSFs) stated in Tanzania's e-Government strategy while meeting all except one of the CSFs proposed by the ISO in its information security management system standard. This evaluation leads to the conclusion that the proposed framework is a robust, sustainable and cost effective framework that is applicable to the government in Tanzania. The proposed framework adds to the body of knowledge in the field of information security as it shows how the Tanzania context of e-Government transactions can be addressed.

(Yildirim, Akalp, Aytac, & Bayram, 2011)

The aims of the study entitled "Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey" were to examine enterprise information security in small and medium-sized enterprises (SMEs) in Bursa, Turkey and to compare the results with similar data gathered from different countries. This study was conducted through questionnaires consisting of 49 questions grouped into 9 sections. The questionnaires were delivered to 97 SMEs in Bursa, Turkey. The companies have been operating for 15.93±11.67 (2–54) years. The number of PCs in the companies and their years of use were in the ranges of 53.51±64.88 (2–240) and 12.47±6.32 (1–30) years, respectively. According to the findings of this study, it can be speculated that when Communications and Operations Management and security policy

improve, other security parameters in the companies, such as Organizational, Personnel and Physical and Environmental Securities improve as well. In addition, the results have shown that Turkish companies do not attach as much importance to information technology security as their counterpart companies from different countries do.

(Ozkan & Karabacak, 2010)

In this case study "Collaborative risk method for information security management practices: A case context within Turkey", a collaborative risk method for information security management has been analyzed considering the common problems encountered during the implementation of ISO standards in eight Turkish public organizations. This proposed risk method has been applied within different public organizations and it has been demonstrated to be effective and problem-free. The fundamental issue is that there is no legislation that regulates the information security liabilities of the public organizations in Turkey. The findings and lessons learned presented in this case provide useful insights for practitioners when implementing information security management projects in other international public sector organizations.

(Kwon, Jang, Lee, & Ki, 2007)

The purpose of this paper "Common defects in information security management system of Korean companies" is to reduce the possible trials and errors while promoting the establishment and certification of the information security management system (ISMS) by enterprises. To satisfy this purpose, this study presents the defects by item found during the certification process of the ISMS of a number of enterprises by government certification agency in Korea. As a result, by analyzing the derived defects, this paper has outlined the issues to be attended to among enterprises at each stage of the establishment of the ISMS. Furthermore, this study presents a reference model for conducting a self-assessment, so that companies may be able to self-verify the completeness of their establishment of the ISMS. The case study is also provided to prove the practical value of this study.

(Luthy & Forcht, 2006)

This research paper titled "Laws and regulations affecting information management and frameworks for assessing compliance" aimed to consider a number of key laws and regulations that have implications for information management and internal control systems. The paper is a discussion of the key laws and regulations. It also considered a number of frameworks that may be useful for assessing compliance with applicable laws and regulations. The paper found that organizations worldwide are impacted by an increasing number of laws and regulations. Many of them have important implications for information management and internal control systems even though they may lack explicit references to information management. This is because information technology (IT) has become pervasive in modern organizations, and it is self-evident that awareness of applicable laws and regulations, along with their potential impacts on information management systems is critical for compliance.

(Hong & Chi, 2003)

This research paper titled "An Integrated system theory of information security management" aimed to build a comprehensive theory of information security management by trying to integrate security policy theory, risk management theory, control and auditing theory, management system theory and contingency theory. Authors suggested that an integrated system theory is useful for understanding information security management, explaining information security management strategies, and predicting management outcomes. Authors also added that few information security strategies and guidelines could be found for practitioners which may result from a lack of coherent and comprehensive information security management theory. Authors found a proposed theory that: (1) Provides rich information security strategies, procedures and theories for researchers, information security decision makers, planners, providers and users; thereby they can get a better understanding of information security in terms of different perspectives. (2) Explains organizational behavior regarding information security management, and provides alternatives for organizational security management strategies. (3) Could be applied to predict the organizational attitudes and behavior towards information security management, and could be beneficial for information

security decision making. (4) Could be a building block for further information security management researcher and be a guidance of future empirical studies.

(Seleznyov & Puuronen, 2003)

This research paper titled "Using continuous user authentication to detect masqueraders" proposed an approach for continuous user authentication based on the user's behavior, aimed to develop an efficient and portable anomaly intrusion detection system. Authors said that a prototype of a host-based intrusion detection system was built, and it detected masqueraders by comparing the current user behavior with his/her stored behavioral model. Authors also added that the model itself is represented by a number of patterns that describe sequential and temporal behavioral regularities of the users. Authors also discussed implementation issues, described the solutions and provided performance results of the prototype. Authors found that there are temporal patterns in user behavior and they may be used as well as sequential ones to efficiently detect anomalies in user behavior. Authors also believed that the temporal may support the anomaly detection, significantly increasing the probability of correct classification. Authors also proposed an efficient way to build and maintain user profiles, keeping resource consumption to a reasonable level.

(Irakleous, 2002)

This research paper titled "An experimental comparison of secret-based user authentication technologies" presents a comparative study of software-based user authentication technologies, contrasting the use of traditional password and personal identifier number (PIN) against alternative methods involving question and answer responses and graphical representation. Authors said that all methods share the common basis of secret knowledge and rely upon the user's ability to recall it in order to achieve authentication. Authors described an experimental trial along with the results based upon (27) participants. They also assessed the alternative methods in terms of practical effectiveness, as well as the perceived levels of user friendliness and security that they provide. Authors concluded that while passwords and PIN approaches garner good ratings on basis of their existing familiarity to participants, other methods based upon

image recall and cognitive questions also achieved sufficiently positive results to suggest them as viable alternatives in certain context.

(Lee & Lee, 2002)

This research paper titled "A holistic model of computer abuse within organizations" in which the authors said that past studies suggest that computer security countermeasures such as security policies, systems, and awareness programs would be effective in preventing computer abuse in organizations. Authors also added: they are based on the general deterrence theory, which posits that when an organization implements countermeasures that threaten abusers, its computer abuse problems would be deterred. Authors proposed a new model of computer abuse that extends the traditional model with the social criminology theories, they focused on computer abuse within organizations, and the model explains the phenomenon through social lenses such as social bonds and social learning. Authors concluded that the new model contributes to our theoretical body of knowledge on computer abuse by providing a new angle for approaching the problem, and it suggests to practitioners that both technical and social solutions should be implemented to reduce the pervasive computer abuse problems.

(Maguire, 2002)

This research paper titled "Identifying risks during information system development: managing the process" attempted to show that there are many areas of potential risk within the process of information system development (ISD) and these need to be carefully analyzed and managed. Author said that certain popular risk management methodologies do not reflect the risk elements identified within the ISD process. Through the case study, the paper has shown that there is a need to develop a risk analysis methodology that incorporates the key issues that need to be addressed before a system goes live. Author added that with risk analysis; the elements of risk have to be isolated at early stage. Author found some potential risk elements which extracted from the case study, some of these elements are multi-tasking capabilities, change several project managers for the development team, lack of rigorous testing, and number of stakeholders.

(Chan & Kwok, 2001)

This research paper titled "Integrating security design into the software development process for e-commerce systems" the authors proposed a software development process for secured systems (SDPSS) based on unified modeling language (UML), in which security design is integrated and means are provided to check whether the security requirements have been incorporated into the final design. Authors used a simplified supply-chain e-commerce system as an example; integration of security design into the software development process is shown with discussions of possible security assurance activities that can be performed on a design.

(Gerber, 2001)

This research paper titled "Formalizing information security requirements" aimed to illustrate that the effectiveness of risk analysis, as a technique used to determine the required level of information security, is no longer adequate to protect modern information resources any longer and to introduce a more modern approach, based on information security requirements. Authors argued that risk analysis, concentrating on assets, threats and vulnerabilities, used to play a major role in helping to identify the most effective set of security controls to protect information technology resources. Authors also added; to successfully protect information, the security controls must not only protect the infrastructure, but also enforce certain security properties in the information resources. To accomplish this; authors said: a more modern top-down approach is called for today, where security requirements driven by business needs state the level of protection required. Authors found a Security Requirements Exercise (SRE) to determine the security requirements which is based on two dimensions. The first dimension is required to consider all factors related to the amount of security necessary for each security concern. The second dimension is used to determine the impacts that unwanted events might have on organizational processes, products and services.

(Hutchinson & Warren, 2001)

This exploratory research paper titled "Attitudes of Australian information system managers against online attackers" aimed to establish a general impression of the

attitudes of Australian professionals in business and government to the concept of "cyber vigilantism". It was undertaken as an initial project to provide the context for a larger, formal international survey. Authors defined the Cyber-vigilantism as the proactive process of responding to information attacks by hackers with corresponding attacks on them. Authors added that, in short, it is hacking the hackers. The research also, explored the policies and procedures which have been set in place by various organizations to cope with concerted attacks on their systems. Authors found that although a majority of managers do approve of the concept of "striking back"; only a minority are prepared for this eventuality. Authors also added that there appears to be complacency about the threats posed by organized, offensive attackers.

(Janbandhu & Siyal, 2001)

This research paper titled "Novel biometric digital signature for Internet-based applications" aimed to introduces the notion of biometric signature – a new approach to integrate biometrics with public key infrastructure, using biometric based digital signature generation which is secure, effective, fast, convenient, non-invasive and correctly identifies the maker of a transaction. Authors said that personal identification numbers, passwords, smart cards and digital certificates are some of the means employed for user authentication in various electronic commerce applications. Authors also added that, these means do not really identify a person, but only knowledge of some data or belonging of some determined object. Author's approach also suggests two schemes for biometric signature using two existing and widely used digital signature algorithms, RSA and (DSA), and discusses the problems associated with them individually. Speed of both schemes (based on iris recognition) is measured and compared with the help of JAVA implementation for both approaches.

(Loukis, 2001)

This research paper titled "Information systems security in the Greek public sector" investigated a set of (53) Greek public sector organizations concerning important aspects of information systems security. Authors stated that the security aspects of public sector information systems are important as the respective systems are often part of

critical infrastructures or deal with personal or sensitive data. Authors found that Greek public sector organizations have only a basic level of information system security awareness. And only a small percentage have developed a systematic, complete, and integrated approach towards the security of their information system, including internal audit procedures. Authors found also that the importance of proper training and generally the importance of the human factor for achieving high levels of information systems security are often underestimated.

(Tsoumas & Tryfonas, 2001)

This research paper titled "From risk analysis to effective security management: towards an automated approach" aimed to describe requirements for a software tool that could assist in the transition from high-level security requirements to a formal, well-defined policy language. Authors said that such a tool would provide valuable assistance and support in both policy implementation and overall security management. Authors also added that one of the various outputs of a risk analysis is a set of recommended practices expressed in high-level statements of a natural language, and in order to be applied to the real world, it is necessary to technically implement those requirements tailored to the specific organizational context. This is usually performed by experienced individuals, authors added. Authors proposed candidate architecture for a policy tool, demonstrating that its implementation is achievable. Authors also argued in this paper that there is a need for further assistance of the security expert's work by automated tools; whether hers/his work can be fully automated is not an issue as such, but it is sure that any contribution eases the burden of the security management.

(White & Pearson, 2001)

This research paper titled "Controlling corporate e-mail, PC use and computer security" conducted by two researchers who inspired to conduct this study because the survey results, which is that corporations began to use computer technology before safeguards were in place regarding its use; and the majority of the company's safeguards continue to be lacking. Not having the control function in place has caused dire consequences for many companies; authors said. The research was limited to control of

personal use of computers, controlling e-mail accounts, and securing company data. Over 200 companies in the south USA were surveyed. The authors found that: (1) A better control in majority of companies is still needed. (2) Company policies regarding personal use of computers are still needed. (3) More monitoring to prevent suits in areas of harassment, libel, and race discrimination is still needed.

(Ye, 2001)

This research paper titled "Robust intrusion tolerance in information systems" discusses causes, chain effects and barriers of intrusions into information systems, and reveal roles that various information security techniques play in intrusion tolerance. Authors said that intrusions exploit vulnerabilities and introduce external disturbances into information systems to compromise security attributes of information systems such as availability, integrity, and confidentiality. Authors also added: Intrusions into information systems cause faults of software and hardware components in information systems, which then lead to errors and failures of system performance. Authors concluded that intrusion tolerance requires information systems to function correctly in a timely manner even under impact of intrusions. Authors presented two robust intrusion tolerance methods through fault masking: Taguchi's robust method for system configuration and sharing of resources via an information infrastructure for redundancy.

(Gritzalis, Iliadis, & Oikonomopoulos, 2000)

The research paper titled "Distributed component software security issues on deploying a secure electronic marketplace" focused on the distributed software security on deploying a secure marketplace. The paper considered a number of distributed component architectures and their security features to support the underlying infrastructure of Secure Electronic Transactions. The paper considered Authentication and Electronic Payment, along with a number of Corporate and Business to Business services are likely to rely heavily on this infrastructure, in order to establish a secure electronic marketplace. The paper also briefly presented TINA, an architecture offering a range of solutions for the up-and-coming transactions involving digital merchandise. After comparing the security issues in three major models in distributed component

software; authors found that: (1) There are a lot of security issues still to be examined in distributed component software systems. (2) Vendors and individual organizations in the electronic marketplace should be expected to improve and implement robust security infrastructures, in order to provide real value for their customers.

(Phukan, 2000)

This research paper entitled with "Ethics and information technology use: a survey of US based SMEs" aimed to study the beliefs and attitudes of small- and medium- sized enterprises (SMEs) toward the ethical use of information technology (IT). Authors used "ethics survey"' conducted in the USA to collect the data they need. Authors found: (1) Even though IT has become an integral part of the US SMEs, there is a clear lack of awareness of basic ethical issues. (2) The participants on this survey did not seem to understand the importance of their moral and ethical responsibilities in the use of IT. (3) Many users pay little or no attention to the laws of software piracy and unauthorized system access.

1.8 Comments on Previous Studies

This study has reviewed (29) studies, (20) foreign studies, and (9) Arabic studies. It also has addressed the issue of information security management and the subject of electronic management, and has varied with each other in addressing these issues from different angles and in different sectors. Some of them dealt with the first domain in this study, namely, information security management (ISM) as one of the variables of the study, in order to reveal its dimensions, elements and its impact on other administrative variables or the effects by these variables, such as: (Gritzalis, Iliadis, & Oikonomopoulos, 2000) study, (Phukan, 2000) study, (Hutchinson & Warren, 2001) study, (White & Pearson, 2001) study, (Gerber, 2001) study, (Chan & Kwok, 2001) study, (Janbandhu & Siyal, 2001) study, (Loukis, 2001) study, (Tsoumas & Tryfonas, 2001) study, (Ye, 2001) study, (Lee & Lee, 2002) study, (Irakleous, 2002) study, (Maguire, 2002) study, (Seleznyov & Puuronen, 2003) study, (Hong & Chi, 2003) study, (Luthy & Forcht, 2006) study, (Kwon, Jang, Lee, & Ki, 2007) study, (Tayeh, Effectiveness of Information Security Management at the Palestinian Information Technology Companies, 2008)

study, (Al-Otaibi, 2010) study, (Ozkan & Karabacak, 2010) study, (Saleh & Alfantookh, 2011) study, (Yildirim, Akalp, Aytac, & Bayram, 2011) study, and (Wangwe, Eloff, & Venter, 2012) study.

Some of them have addressed the second domain in this study, namely, electronic management, such as: (Al-Ajez, 2011) study, (Al-Aloul, 2011) study, (Al-Somairy, 2009) study, (Ammar, 2009) study, (Zoarob, 2009) study, and (Al-Ghoty, 2006) study.

It is clear from what has been shown previously that the topic of information security management (ISM) and the subject of electronic management have gained the attention of researchers, although they may have been dealt with separately. It was found through a review of previous studies that:

- Part of these studies has targeted the definition of information security management, through important aspects of this domain, in an effort to a deep understanding of its constituent elements.

- The other part of these studies has targeted the identification of e-management in order to a deep understanding of its constituent elements, the factors affecting it, the needed requirements to apply it, and constraints that limit its presence, and then, to explain what surrounds this concept of ambiguity, and translate its elements and vocabulary to suit the work in administrative field.

- These studies were conducted in different environments, some of them were conducted in foreign environments and others were conducted in Arabic ones, as some of them were conducted in public sectors, and others were conducted in private sectors.

- Previous studies have helped in guiding the development of this study theoretical framework and determining the appropriate statistical methods to analyze the study data.

- The contribution of these studies in supporting the administrative development in the institutions and departments, as one of the continuity and survive factors

under the great development, rapid and dramatic changes in the sectors of knowledge and technology, in an effort to keep pace with these rapid changes in the various fields to raise their efficiency and effectiveness.

- These studies differ among themselves, and within each domain in terms of dimensions, elements and variables that have been focused by each study, leaving the field wide and open for researchers to fill the research gaps and to contribute to the enrichment of the knowledge and practical sides of both domains of this search.

What distinguishes the current study from previous studies?

- It is the first study in the local environment, to the knowledge of the researcher, dealing with information security management as a strategic approach for the effective applying of e-management in the governmental institutions in Gaza.
- It is unique to study the relationship between the elements of information security management (Security Policy, Organizational Security, Assets Classification and Control, Personnel Security, Physical and Environmental Security, Computer and Network Management, System Access Control, System Development and Maintenance, Business Continuity Planning, Compliance to Legal Requirements) and the effective applying of electronic management.
- It highlights the e-management environment, to increase the interest in it, and to create the right climate to increase the effectiveness of performance, and to issue the necessary recommendations to fill the gaps that hinder the effective implementation of the electronic management in the Governmental institutions in Gaza.
- This study highlights the weak fields of information security management in the Governmental institutions in Gaza.

CHAPTER (2)

INFORMATION SECURITY MANAGEMENT

We must plan for freedom, and not only for security, if for no other reason than that only freedom can make security secure (Popper, 1945).

"An information security digital divide between users and information security managers with regard to skills, knowledge and responsibilities is therefore to be expected" (Albrechtsen & Hovden, 2009).

2.1 Introduction

This chapter examines the nature of the present-day approach to information security management (or information security management system) in the organization. Information security management (ISM) is implemented in the organization through the organizational structure of an information security management system (ISMS); consequently, this thesis treats the terms ISM and ISMS synonymously. The analysis in this chapter attempts to discover whether the non-compliance of end-users can be traced back to the managerial style of information security managers in the organization. The next two sections will discuss the role, and importance of information security management in the organization and its process. The subsequent two sections will discuss the evolution of information security and the problems associated with present-day information security management systems. This chapter firmly establishes that the present-day approach to information security management in the organization is bureaucratic in nature and thus, by implication, largely responsible for the non-compliance exhibited by the end-users in the organization (Rastogi, 2011).

2.2 Defining information security

In order that the terminology used in this study is clearly understood, a selection of key terms is defined here. Before delving any further, it is vital that the term security be clearly defined. What does *security* commonly referred as computer security mean? Moreover, what does *information security* mean? A review of the various sources of computer related terms including (SANS Institute, 1998), (TechTV, 2001a), and (Webopedia, 2002) revealed numerous and diverse definitions of these terms indicating that there are no widely agreed upon definitions.

The first definition of *security* is by (Webopedia, 2002)

Security refers to techniques for ensuring that data stored in a computer cannot be read or compromised.

The second definition of security is by (SANS Institute, 1998)

Security: A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.

The definition of computer security above implies that organizations need to know the value of information and how it can be compromised in order to develop protective measures. There is a general consensus as to the meanings of the terms: availability, integrity and confidentiality.

- *Availability*. The prevention of unauthorized withholding of information or resources. This does not apply just to personnel withholding information. Information should be as freely available as possible to authorized users.
- *Integrity*. The prevention of erroneous modification of information. Authorized users are probably the biggest cause of errors and omissions and the alteration of data. Storing incorrect data within the system can be as bad as losing data. Malicious attackers also can modify, delete, or corrupt information that is vital to the correct operation of business functions.
- *Confidentiality*. The prevention of unauthorized disclosure of information. This can be the result of poor security measures or information leaks by personnel. An example of poor security measures would be to allow anonymous access to sensitive information.

The third definitional statement of computer security is by (Howard, 1997)

Computer security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks.

The first definitional statement of information security is by (SANS Institute, 1998)

Information security is a system of procedures and policies designed to protect and control information

Compounding the definitional problems of computer security is that it is viewed essentially as being synonymous with information security although their meanings differ as seen from the definition by (SANS Institute, 1998) below.

Information Security: The result of any system of policies and/or procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute.

In the above definition, information security is distinguished from computer security in that it is a goal whereas computer security is a means toward a goal: information security.

From the definitions above, two key points stand out:

(1) Talking about security implies talking about entities of a technological nature.

(2) Information is the key most important asset that needs protection.

The definitions above are also useful in bringing out the problem of the distinction between security and a host of other security related terms. The distinction is far from being clear-cut. As such, security is often used interchangeably in the literature to mean computer security, Internet security, network security and information security (Goh, 2003).

2.3 The role of information security management

According to (von Solms , 2001), information security is a multidimensional discipline. One of the dimensions of information security is the 'Governance / Organizational dimension'. This dimension refers to the way that information security is organized, structured and managed in an organization. According to (von Solms , 2001), information security management is an important dimension underlined by the availability of various international best practices, standards and guidelines which all stress the importance of an organizational structure for information security. The 'Governance/Organizational' dimension of information security establishes information

security related job roles and responsibilities, communication between these roles and top management commitment and involvement with information security in the organization. Eloff & Eloff (2003) define an information security management system (ISMS) as *"a management system used for establishing and maintaining a secure information environment"*. The ISMS establishes the processes and procedures required to manage information security. The aim of these processes and procedures is to preserve the security of the information assets of the organization and to work towards the continual improvement of information security in the organization (Posthumus & von Solms, 2005). The international standard on ISMS, ISO/IEC 27001:2005 (ISO/IEC 27001, 2005) defines information security management system as *"that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security"*. In a note to the definition, it says that *"the management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources"* (ISO/IEC 27001, 2005).

ISMS can be viewed from different perspectives (Eloff & Eloff, 2003):

- Strategic perspective: addressing corporate governance, policies and pure management issues;
- Human perspective: addressing security culture, awareness, training ethics and other human related issues;
- Technology perspective: addressing issues related to hardware and software products; and
- Process perspective: addressing the implementation of controls as contained in a standard or code of practice and the compliance with these controls.

Eloff & Eloff (2003) further state that information security management should take a holistic approach consisting of the integration of all the four perspectives in implementing ISMS in the organization. Information security management in an organization plays a vital role in establishing an environment of information security in the organization. Through its organizational structures, processes and procedures, the ISMS attempt to preserve the security of vital information assets of the organization. As

stated by (Eloff & Eloff, 2003), the ISMS has a human side as well. The next section discusses how information security management operates in the organization (Rastogi, 2011).

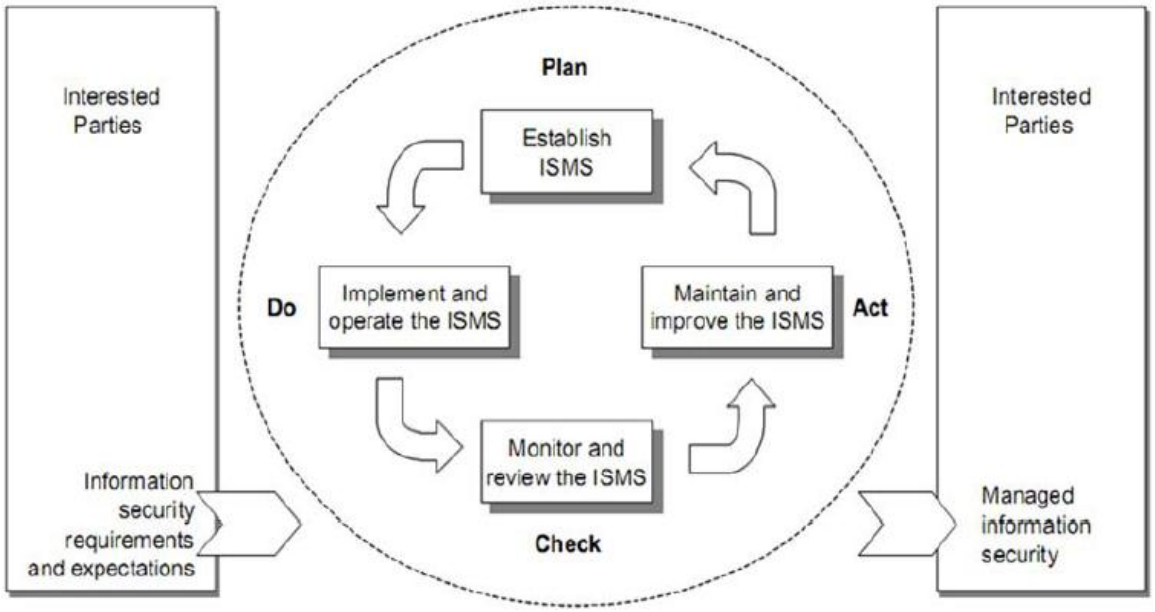
2.4 The process of information security management

Eloff & Eloff (2003) state that the process of ISMS consists of two phases, namely, planning and then implementing management practices, procedures and processes for establishing and maintaining information security. According to (Posthumus & von Solms, 2005), the ISMS process consists of:

- Obtaining clear direction from guidance available in security standards or codes of practice. Additional guidance is available from the corporate information security policy.
- Assessment of various potential risks to the information.
- Formulation of a risk management strategy resulting in the identification and implementation of physical, technical and operational security controls.
- Staff training in security practices.
- Testing the security infrastructure.
- Detecting and responding to security incidents.
- Auditing the security function and reporting to the board on its effectiveness.

ISO/IEC 27001:2005 (ISO/IEC 27001, 2005) adopts a ‘process approach’ for implementing ISMS in the organization. This process approach consists of the Plan-Do-Check-Act (PDCA) model (see Fig. 2.1).

Figure (2.1): PDCA Model applied to ISMS Processes



(ISO/IEC 27001:2005).

As shown in Figure (2.1), the ISMS takes as input the information security requirements and expectations from the interested parties and then delivers managed information security to these parties. This transformation from needs to managed security takes place through the operation of the ISMS. The process provided in ISO/IEC 27001:2005 for establishing and maintaining the ISMS is as follows (also see Table 2.1):

- Establish the ISMS: identify its scope; analyze the risks; select control objectives and controls; obtain management authorization to implement and operate the ISMS.
- Implement and operate the ISMS: implement the controls; implement training and awareness program; manage operation and resources for the ISMS.
- Monitor and review the ISMS: review and measure the effectiveness of controls and the ISMS; conduct internal ISMS audits.
- Maintain and improve the ISMS: implement identified improvements in the ISMS and inform all interested parties; ensure that improvements achieve the intended results.

Table (2.1): PDCA Model for ISMS

Plan (establish the ISMS)	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do (implement and operate the ISMS)	Implement and operate the ISMS policy, controls, processes and procedures.
Check (monitor and review the ISMS)	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act (maintain and improve the ISMS)	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

(ISO/IEC 27001:2005).

The companion standard ISO/IEC 27002:2005 (ISO/IEC 27002, 2005) provides further guidance for the training and awareness program for employees of the organization. The standard says that during the period of their employment, it is the management's responsibility to ensure that all employees or users of the organization are provided with guidance, training and education regarding the sensitivity of the information they handle and the policies and procedures in place. The standard further states that there should be a formal disciplinary process for employees who commit a security breach.

von Solms & von Solms (2004) have listed the factors crucial to the success of ISMS in an organization. These factors have been labeled as 'sins' since missing these factors severely affects the effectiveness of ISMS implementation. These factors are:

- Not realizing that information security is a corporate governance responsibility (the buck stops right at the top).
- Not realizing that information security is a business issue and not a technical issue.

- Not realizing the fact that information security governance is a multi-dimensional discipline (information security governance is a complex issue, and there is no silver bullet or single 'off the shelf' solution).
- Not realizing that an information security plan must be based on identified risks.
- Not realizing (and leveraging) the important role of international best practices for information security management.
- Not realizing that a corporate information security policy is absolutely essential.
- Not realizing that information security compliance enforcement and monitoring is absolutely essential.
- Not realizing that a proper information security governance structure (organization) is absolutely essential.
- Not realizing the core importance of information security awareness amongst users.
- Not empowering information security managers with the infrastructure, tools and supporting mechanisms to properly perform their responsibilities.

Similarly, ISO/IEC 27002:2005 (ISO/IEC 27002, 2005) has listed critical success factors for ISMS implementation. These are:

- Information security policy, objectives, and activities that reflect business objectives;
- An approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the organizational culture;
- Visible support and commitment from all levels of management;
- A good understanding of information security requirements, risk assessment, and risk management;
- Effective marketing of information security to all managers, employees, and other parties to achieve awareness;
- Distribution of guidance on information security policy and standards to all managers, employees and other parties;
- Provision to fund information security management activities;

- Providing appropriate awareness, training, and education;
- Establishing an effective information security incident management process;
- Implementation of a measurement system that is used to evaluate performance in information security management and feedback suggestions for improvement.

At this point, in relation to the problem of end-user non-compliance, it is vital to note that the near total neglect by the present-day approach to ISM is regarding to the consideration of the human aspect of information security. The present-day approach to ISM, as evidenced by the role and process of ISMS discussed above, treats end-users in a rather simplistic manner – it assumes that compliance of end-users to information security policies and controls in the organization can simply be achieved by improving the awareness and skill levels of end-users. Beyond this, if end-user non-compliance persists, then end-users are to be blamed and treated through a disciplinary process. Against this backdrop, the later sections discuss the evolution of information security (Rastogi, 2011).

2.5 Building an information security plan

A complete security program must address the business information and the security process. A security plan must be reasonable and prudent for the organization. What is a reasonable and prudent level of security depends on many things, including the type of information being protected, the type of business being conducted, and with whom the business is being conducted. Industry and governmental regulations will also define some of the security measures that are required as a minimum (Pipkin, 2000).

An information security plan is a large undertaking. It encompasses risk analysis, business impact analysis, disaster planning, and business continuity plans. It addresses the core business processes throughout the organization and requires the support of all the business units.

The information security plan is composed of four main components. The business impact analysis defines the scope of the information security plan and those information assets that have the greatest impact on the business processes. The risk analysis defines the probability of harm and the extent of the possible damage. Disaster

planning evaluates the best method to minimize the effects of harm. It identifies the functions needing quickest recovery, and establishes the recovery strategies. The business continuity plan is concerned with not only what to do when there is a disaster, but how to continue to conduct business at all times, disaster or not (Pipkin, 2000).

An information security plan brings together all of these issues. It identifies critical business processes (those processes required for organization's survival), determines the necessary resources to perform each process, and evaluates the impact of an interruption to the process. It determines the costs of assuring a minimum quality of service, develops into a plan to meet this level of service, and puts into place the processes needed to deploy the plan.

Organizations can no longer regard security as an option, only needed for government contracts. Today's business environment makes security a requirement without which the organization will most certainly suffer damaging losses. The information security plan must be integrated into the core business planning and review process. This keeps information security visible to senior management during all phases of the planning process. It also simplifies the process of having senior management reviews and endorses the plan, since they have been involved during the planning process (Pipkin, 2000).

The five main phases of an information security plan are as follows (Pipkin, 2000):

Inspection – The most important tasks in developing an information security plan are identifying the key corporate functions, the capabilities they need, when they need those capabilities, and how they interact with other functions. The inspection phase evaluates the security needs of the organization, as well as its current level of preparation.

If systems were built with care and good software engineering practice, we would have a greatly reduced problem with information security. (Spafford, 1999)

Protection – Proactive risk reduction includes any process that is in place to prevent a business interruption such as identifying and qualifying second source, purchasing spare equipment, expanding product pipeline duration, backing up critical documentation, and

outsourcing operations if necessary. This is accomplished by creating a comprehensive security design.

Government and commercial computer systems are so poorly protected that they can essentially be considered defenseless: an electronic Pearl Harbor waiting to happen. (Schwartau, 1991)

Detection – Reactive risk reduction includes any process that is in place to minimize the losses from an incident that could cause an interruption of business process. This phase explores the process of detecting misuses by examining the attacker, the methods of attack, and the technologies that are used to detect them.

I'm not concerned about the vulnerabilities that I know about – I've already taken precautions against them – it's the ones that I don't know about that have me worried. (Ranum, 1995)

Reaction – The emergency response plan determines how to respond when there is a security incident. It must define the process of responding to probable scenarios. The response must be identified, documented, and tested before there is an incident so that everyone knows what to do during the crisis. The incident response plan is a critical part of the business continuity plan. Preparation is key to a successful response.

The biggest mistake people make is they underestimate the threat. (Moss, 1998)

Reflection – When the security incident is over and the smoke clears, the organization must perform follow-up steps to be able to put the incident behind and move forward. The processes that need improvement will undoubtedly be processes that are defined in the business continuity plan. As these improvements are evaluated, a big picture view is needed to see if there are other areas of the business continuity plan to which these changes would be beneficial, or if the changes would affect other areas of the plan.

We are now worse off, with respect to protecting our critical infrastructure, than we a few years ago. (Schultz, 1999)

Every organization needs to review its information security plans. During this process many will discover that their business plans do not address the issue of information security. Global security direction must be created for the organization so that specific policies can be built in a consistent manner (Pipkin, 2000).

2.6 The four waves of information security

Since its inception, some decades ago now, information security and its management have continued to evolve. Von Solms (2000 & 2006) describe this evolution in terms of four waves. These waves are: the technical wave, the management wave, the institutionalization wave and the governance wave (von Solms, 2000) (von Solms, 2006). Von Solms (2000) presented the first three waves while Von Solms (2006) presented the fourth wave. This section presents an overview of these waves of development as presented in (von Solms, 2000) (von Solms, 2006).

The first wave is the technical wave which lasted until the early eighties and represents the highly technical approach to information security. This was the era of mainframe-based computing and highly technical users. In this era, information security consisted largely of securing the IT assets through the use of built-in access control lists, user-ids and passwords. People-related aspects such as information security policies, information security awareness of users etc. were not even acknowledged. Information security was a technical issue and dedicated to the needs of technical people. However, the responsible people for implementing information security began to realize that this approach was not appropriate and that they needed management's commitment and involvement to guarantee the effectiveness of information security.

The second wave is the management wave which lasted from the early eighties to the middle nineties. This wave is characterized by the growing management realization of the importance of information security to the survival of the organization and the consequent involvement of management in the implementation of information security. The era of the second wave coincided with the development of organizational computing from mainframe-based computing to the distributed computing and the arrival of technologies such as the Internet, WWW and E-commerce. As these technologies became

more and more important for the organizations, information security too gained prominence and the top managements of organizations began to get involved. Information security policies, information security managers and organizational structures for information security were established. As top management has become involved with information security, the information security people not only got the sanction to go ahead with securing the organization's information assets, but they also got questioned about issues such as progress and results. Information security managers were saddled with the responsibility of drafting policies and procedures, and they started to report to top management through organizational structures.

The second wave overcame some of the shortcomings of the first wave and management involvement led to improvements in the effectiveness of information security in the organization. However, now organizations wanted to know how well they were doing in their information security efforts and how they could benchmark themselves against other organizations. Another significant realization was that the human aspect of information security was perhaps the biggest impediment to the effectiveness of information security in the organization.

The third wave began in the late nineties and lasted until the mid-2000s when the fourth wave began. This is the wave of the institutionalization of information security. This wave is characterized by aspects like best practices and codes of practice for information security management, international information security certification, cultivating information security as a corporate culture, and dynamic and continuous information security measurement. The third wave filled the gap that was felt in the second wave, namely, that of the availability of guidance for the implementation of information security in the organization. The third wave consisted of the following components, each component addressing a particular syndrome:

- Information Security Standardization: availability of guidance in the form of international best practices addressing the syndrome *"how do I know I am not missing something?"*

- International Information Security Certification: availability of audit and certification bodies to address the twin syndromes of *"how do I prove my security preparedness to an E-commerce partner?"* and *"how can I allow a potential E-commerce partner into my system if I know nothing about his information security preparedness?"*
- Cultivating an information security culture throughout an organization: this consists mainly of comprehensive information security awareness programs and addressed the syndrome *"my own users may be my biggest enemy?"*
- Implementing metrics to continuously and dynamically measure information security aspects in an organization: this consists of continuous measurement of the state of information security in the organization and addresses the syndrome *"how do I know how well our information security policies, procedures etc. are complied with?"*

The third wave, in parallel with the first and second waves, established a more mature discipline of information security. The technical measures of the first wave and the managerial involvement of the second wave were supplemented by guidance in the form of standards and certifying bodies. Additionally, the implementation of information security was further enhanced with the introduction of culture and awareness programs in recognition of the importance of people for information security.

The fourth wave began in the mid-2000s and consists of the development of information security governance. This is the era in which IT has become pervasive and is crucial to the operation, growth and survival of organizations. This dependence has led to developments in the field of corporate governance which make top management and boards of directors of organizations directly responsible for the health and security of their IT systems. Consequently, the responsibility for information security in the organization has risen to the top echelons of the organization. This has led to information security governance becoming an integral part of corporate governance. The fourth wave is characterized by another crucial realization, namely, that the use of IT systems by humans, i.e. employees, clients and customers, can lead to serious information security risks. Organizations and their management have realized that technical measures alone

cannot solve this problem and that this requires strategic decisions at a high-level to improve the awareness of all the end-users.

The four waves in the development of information security, as put forward by (von Solms, 2000) (von Solms, 2006) represent a maturing of the information security discipline. These waves operate in parallel and, together, these developments ensure that not only technical means and controls are available for information security, but policies, procedures and guidance in the form of best practices and standards are also available for practitioners. Furthermore, organizations can measure and benchmark their information security efforts. These waves have seen the responsibility for information security escalate from the technical IT staff to the top echelons of the organization. Another important aspect has been the realization regarding the importance of user awareness and compliance to the effectiveness of information security. This has led to the development of awareness programs and efforts to create an information security culture in the organization such that information security becomes a way of life for the people in the organization.

As stated previously, information security management has tended to take a simplistic approach to end-users. This fact is further reinforced by the delineation of the evolution of information security through the four waves. The behavior of people (as employees or end-users) in the organization is complex and, hence, requires a comprehensive managerial approach. (Rastogi, 2011).

2.7 The bureaucratic nature of present-day ISMS

This section discusses the incompleteness or the shortcomings of the present-day approach to ISM in regard to the management of end-users aspects of information security. The earlier discussions have prepared the grounds as follows (Rastogi, 2011):

- End-user compliance with information security policies and controls is crucial to the success of information security in the organization. End-user non-compliance has the potential to lead to information security breaches. Further, this non-compliance emerges from a cluster of factors which are not entirely under the control of end-users. Consequently, it may be inappropriate to blame end-users

alone and the remediation of non-compliance requires a more comprehensive approach.

- The managerial style in an organization has a significant influence on the employee behavior in the organization. Managerial styles based on Theory X assumptions of human nature, such as scientific management or bureaucracy, lead to the erosion of commitment and an unhealthy work culture. Alternative managerial styles, such as those based on Theory Y assumptions, lead to a more committed work force.
- Information security management plays a vital role in the establishment of information security in the organization. However, even as information security has evolved, and even as there are international standards and best practices guiding the implementation of information security in the organization, only a very narrow approach is adopted towards dealing with end-users in information security. The major aspect of the approach towards end-users may be summarized as follows: provide awareness and training to end-users to enable them to comply; if non-compliance persists then treat it through a disciplinary process.

The present-day approach of ISM is reminiscent of scientific management and bureaucracy. Hence, it may be that the present-day approach is, in fact, contributing to end-user noncompliance, rather than restraining it.

Frangopoulos (2007) states that today's ISMS can be characterized by the following features:

- Use of rules and regulations aiming to provide a secure environment.
- Commitment of everyone involved to a set of prescribed guidelines, i.e. behavior control.
- Use of technical measures for controlling the application of rules and regulations and the upholding of behavior control.
- Use of non-technical measures to complement the technical measures.

Albrechtsen (2008) provides a similar analysis of present-day ISMS. He concurs that present-day ISMS is bureaucratic in nature and it can be characterized as follows:

- Use of technology to control and monitor user behavior in addition to function as a secure system.
- Use of documented descriptions of expected individual and organizational behavior.
- Use of formal, one-way communicated, expert-based training and education of employees.
- Modest involvement of employees in the information security work.
- Lack of dialogue and interaction between information security professionals and users.
- Centralized management, with expert knowledge on information.

Albrechtsen (2008) states that bureaucratic ISMS suffers from two problems:

- Its inability to adjust to the dynamic nature of IT, organizations and threats.
- It is inappropriate for handling the human aspect of information security.

According to (Albrechtsen, 2008), traditional management is based on the use of technological and bureaucratic means for the control of users. He states that present-day ISMS represents a paradox since it attempts to manage the security of modern and dynamic IT through traditionally structured approaches and perspectives.

Albrechtsen (2008) explored the relationship between users and information security managers. His study indicates the divide between users and information security management. The results were as follows:

- Documented rules and guidelines have only a limited effect on users' information security behavior.
- Uses feel that information security managers are invisible and inaccessible.
- Users experience their interactions with information security managers as expert-based, top-down interactions with no or moderate involvement of users.

- Users' perceptions of risk differ from those of information security managers.

  Ashenden (2008) states that the role of information security managers in an organization is that of a technical specialist and that information security management is approached in a 'command and control' style. Information security is treated as a technical subject and best managed by technical staff. In pursuance of this approach, information security managers tend to ignore the end-users – *"they focus on talking, presenting and reinforcing ideas"* and *"not listening to end-users"* (Ashenden D. , 2008). The neglect of end-users is further reinforced by incorrect perceptions as information security managers do not engage with end-users and they do not try to understand how end-users perceive information security; rather, information security managers rely on *"how they think"* end-users perceive information security. Ashenden (2008) states that this view is *"unlikely to be neutral"*.

Sensing the difficulties as discussed above, Dhillon (2001a) has provided the principles for information security management more suitable to today's needs. These principles are:

- Principles for managing the pragmatic aspects
  - ✓ Education, training and awareness, although important, are not sufficient conditions for managing information security. A focus on developing a security culture goes a long way in developing and sustaining a secure environment.
  - ✓ Responsibility, integrity, trust and ethicality are the cornerstones for maintaining a secure environment.
- Principles for managing the formal rule-based aspects
  - ✓ Establishing a boundary between what can be formalized and what should be norm based is the basis for establishing appropriate control measures.
  - ✓ Rules for managing information security have little relevance unless they are contextualized.
- Principles for managing the technical systems

- ✓ In managing the security of technical systems, a rationally planned grandiose strategy would fall short of achieving the purpose.
- ✓ Formal models for maintaining the confidentiality, integrity and availability (CIA) of information cannot be applied to commercial organizations on a grand scale. Micromanagement for achieving CIA is the way forward.

In the principles proposed by (Dhillon, 2001a), it is stated that awareness and skills alone are insufficient for ensuring compliance by end-users. A more comprehensive approach is needed, based on a richer role for end-users in the organization. Furthermore, information security policies and controls need to be contextualized.

Finally, Schlienger & Teufel (2002) underline the problem with today's approach to information security management. According to (Schlienger & Teufel, 2002), the problem lies in the conception of the human dimension of information security. In the present-day, information security management is mainly focused on technical measures.

In this approach, the users are seen as a threat. There is distrust between information security management and users. In this scenario, information security management treats users as the *"enemy"* and there is no inclination to discuss the human aspect of information security. However, Schlienger & Teufel (2002) also propose a solution to this imbroglio. According to (Schlienger & Teufel, 2002), the solution lies in information security management undergoing a paradigm shift in regard to its conception of the human dimension. Information security management needs to shift from a technical to a human-centric focus. This approach requires a cultural change in information security management. In the new approach, the user is no longer the enemy; rather, the user becomes a *"security asset"* (Schlienger & Teufel, 2002). As Schlienger & Teufel (2002) put it, the new information security management approach should be *"a socio-cultural, human centric approach that is based on trust and partnership, accompanied by appropriate security technology"*.

This section has firmly established the bureaucratic nature of the present-day approach to information security management. This means that the non-compliance of end-users can be traced back to information security management itself. Authors such as

Dhillon, Schlienger and Teufel have provided a way forward from this malaise – that of a human-centric approach to information security management in the organization.

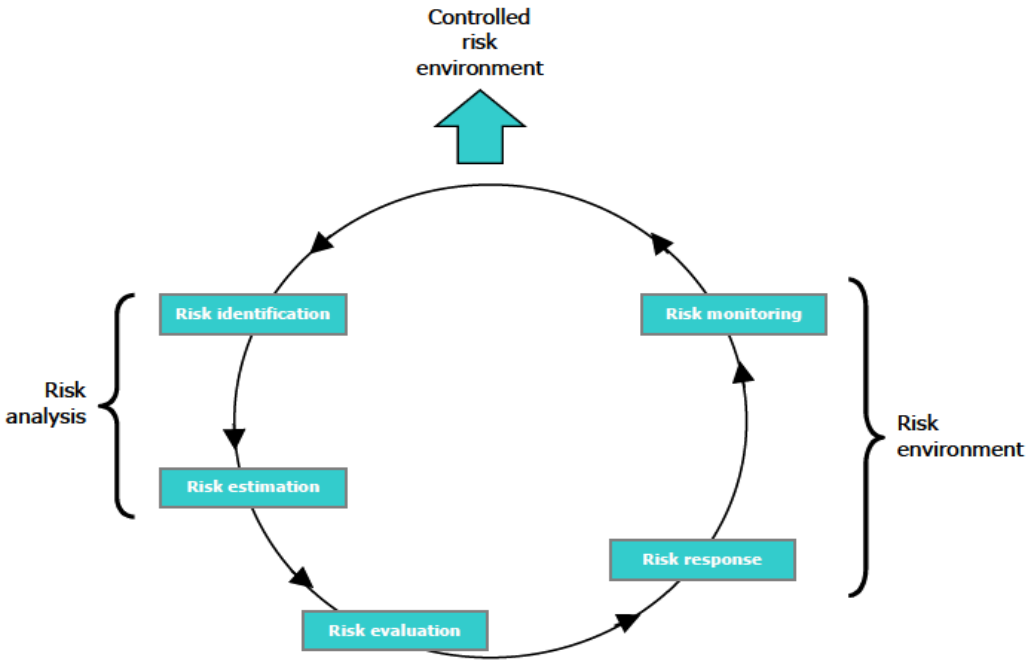
2.8 Governance, Risk Management and Compliance

Managing governance, risk and compliance across the enterprise is a challenging proposition. To address this issue, a class of solutions known as GRC (governance, risk management and compliance) has sprung up. In addition, many enterprises will end up developing and implementing custom solutions that they build in-house. However, coming up with the right requirements for the appropriate GRC solution is a complicated undertaking. Every enterprise will have unique needs that will drive what the GRC solution should look like. These needs might be the compliance regiment that the enterprise has to adhere to the threats faced by it, its risk appetite or a multitude of other considerations. No formal models exist that help the definition of an enterprise's GRC needs (Singh, 2009).

2.9 General risk management approaches

An organization is exposed to a staggering array of risks, whether they are information risks, operational risks or financial risks. A general procedure to manage risk, consist of five phases: identification, estimation, evaluation, response and monitoring (see Fig. 2.2).

Figure (2.2): Risk management cycle



(Baker, Ponniah, & Smith, 1998).

To obtain a controlled risk environment, organizations need to first identify the threats that constitute risk to the organization and then estimate the risk. These two steps comprise the important risk analysis, which every organization should put time and effort to. Next step is the risk evaluation phase, which evaluate to what extent the risk might affect the business. The last two steps are about risk control and include risk response and risk monitoring. The organizations need to decide how to manage the risks and then monitor that the preventing actions comply with the intentions (Baker, Ponniah, & Smith, 1998).

Regardless of how complex and varied the risks within the organization are, an organization has four possible fundamental approaches to manage a given risk. It can avoid risk, reduce risk, transfer risk or retain risk. The first two approaches minimize a organization's overall exposure to risk and they are sometimes referred to as risk control. The two later approaches are known as risk financing and the goal for those is to ensure

that funds are available to cover losses that do occur after the application of risk control techniques (Shimpi, 1999).

2.9.1 Risk avoidance

An organization can elect to abstain from investments with payoffs that are too uncertain (Shimpi, 1999). Thus, the risk can be avoided by not undertaking activities that are risky or by substituting less risky process (Hussain, 2000). Each organization has to draw a line between acceptable and unacceptable risks and the decision concerning where this line should be drawn depends on a combination of internal and external factors. Risk avoidance reflects each firm's need to maintain focus and pick its battles (Shimpi, 1999).

2.9.2 Risk reduction

Risk reduction occurs through loss prevention, loss control and diversification. Loss prevention seeks to reduce the likelihood of a given type of loss occurring and examples of loss prevention measures include safety devices like smoke detectors and burglar alarms (Hussain, 2000) (Shimpi, 1999). Loss control techniques are designed to reduce the severity of a loss, should it occur. Sprinkler systems and firewalls for example, limit the damage if a fire would take place (Hussain, 2000) (Shimpi, 1999). Also, an organization can limit its downside risk of a project by inspections, closely monitoring its progress and regularly evaluating its efficiency, which is a loss control technique as well (Shimpi, 1999). Diversification provides a third mean of reducing risk, which has crystallized over the past half-century with Markowitz's development of the portfolio theory. It offers an opportunity to spread out the risk without sacrificing the expected return (Brealey & Myers, 2000) (Shimpi, 1999).

2.9.3 Risk transfer

The risk can also be transferred from one party to another better equipped or more willing to bear it (Shimpi, 1999). For example, the risk can be transferred to counterparty by purchase of an insurance policy or financial hedge (Hussain, 2000).

2.9.4 Risk retention

Companies also retain a variety of risks, whether voluntarily or involuntarily, i.e. in an active or passive way. Voluntary risk retention reflects a conscious decision to absorb certain risk exposures internally, because it is the most cost-efficient way of addressing the risk. Involuntary risk retention occurs when a business fails to identify a given risk exposure and therefore bears the risk unknowingly. A risk neglected is a risk retained, or simply not insuring is retaining risk (Hussain, 2000) (Shimpi, 1999) (Brag & Wedefelt, 2004).

2.10 Web services security

Perhaps the most precise and practical definition of the term web services (WS) is provided by the W3C Web Services Architecture Working Group: "A web service is a software application identified by a URL, whose interfaces and binding are capable of being defined, described, and discovered as XML artifacts. A web service supports direct interactions with other software agents using XML-based messages exchanged via Internet-based protocols" (W3C, 2004) (Ferrari & Thuraisingham, 2006).

WS are distributed, decentralized, self-contained, self- describing; can be dynamically published, located, invoked; are language independent and interoperable, inherently open, standards based; and are able to be composed and provide well-defined services to certain services consumers (Endrei, et al., 2004). Consequently, WS based-solutions must be concerned with typical security problems that are common to distributed communications, through a compromised channel, between two or more parties. Some of the major inherited security issues that WS technologies must address are authentication, authorization, confidentiality, data integrity, non-repudiation, and availability (Sedukhin, 2003). WS must address both the issues inherited from the distributed computing classical scheme and those arising from the new threats created by its own nature (Ferrari & Thuraisingham, 2006).

In addition, ways to protect services providers and services consumers are needed. For example, service providers can be protected by applying control access mechanisms to the services (OASIS, 2003b) or information (Shandu, Coyne, Feinstein, & Youman,

1996) they own or by guaranteeing non-repudiation of the interactions they perform. On the other hand, service consumers' protection is mainly focused on service trustworthiness and data privacy concerns. Service trustworthiness assures service consumers that the service they plan to use will act as expected (e.g., as indicated in the related meta-information). Data privacy deals with protecting sensitive and personal information collected by a service from unauthorized disclosures (Ferrari & Thuraisingham, 2006).

2.11 ISO/IEC 27000-series

The **ISO/IEC 27000-series** (also known as the 'ISMS Family of Standards' or 'ISO27k' for short) comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) (ISO/IEC 27001, 2005) (ISO/IEC 27002, 2005).

The series provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series).

The series is deliberately broad in scope, covering more than just privacy, confidentiality and IT or technical security issues. It is applicable to organizations of all shapes and sizes. All organizations are encouraged to assess their information security risks, and then implement appropriate information security controls according to their needs, using the guidance and suggestions where relevant. Given the dynamic nature of information security, the ISMS concept incorporates continuous feedback and improvement activities, summarized by Deming's "plan-do-check-act" approach, that seek to address changes in the threats, vulnerabilities or impacts of information security incidents. The standards are the product of ISO/IEC JTC1 (Joint Technical Committee 1) SC27 (Sub Committee 27), an international body that meets in person twice a year.

At present, eleven of the standards in the series are published and available, while several more are still under development. The original ISO/IEC standards are sold

directly by ISO, while sales outlets associated with various national standards bodies also sell various versions including local translations.

2.11.1 Published standards

- ISO/IEC 27000 — Information security management systems — Overview and vocabulary.
- ISO/IEC 27001 — Information security management systems — Requirements
- ISO/IEC 27002 — Code of practice for information security management
- ISO/IEC 27003 — Information security management system implementation guidance
- ISO/IEC 27004 — Information security management — Measurement
- ISO/IEC 27005 — Information security risk management
- ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27010 — Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications
- ISO/IEC 27011 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27031 — Guidelines for information and communications technology readiness for business continuity
- ISO/IEC 27033-1 — Network security overview and concepts
- ISO/IEC 27035 — Security incident management
- ISO 27799 — Information security management in health using ISO/IEC 27002

2.12 ISO/IEC 27001

ISO/IEC 27001, part of the growing ISO/IEC 27000 family of standards, is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC). Its full name is *ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements*.

ISO/IEC 27001 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified compliant with the standard (ISO/IEC 27001, 2005) (ISO/IEC 27002, 2005).

2.12.1 How the standard works

Most organizations have a number of information security controls. However, without an information security management system (ISMS), controls tend to be somewhat disorganized and disjointed, having been implemented often as point solutions to specific situations or simply as a matter of convention. Security controls in operation typically address certain aspects of IT or data security specifically; leaving non-IT information assets (such as paperwork and proprietary knowledge) less protected on the whole. Moreover business continuity planning and physical security may be managed quite independently of IT or information security while Human Resources practices may make little reference to the need to define and assign information security roles and responsibilities throughout the organization.

ISO/IEC 27001 requires that management:

- Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
- Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

The Key Benefits of 27001 are:

- It can act as the extension of the current quality system to include security
- It provides an opportunity to identify and manage risks to key information and systems assets

- Provides confidence and assurance to trading partners and clients; acts as a marketing tool
- Allows an independent review and assurance to you on information security practices

An organization may want to adopt ISO 27001 for the following reasons:

- It is suitable for protecting critical and sensitive information
- It provides a holistic, risked-based approach to secure information and compliance
- Demonstrates credibility, trust, satisfaction and confidence with stakeholders, partners, citizens and customers
- Demonstrates security status according to internationally accepted criteria
- Creates a market differentiation due to prestige, image and external goodwill
- If an organization is certified once, it is accepted globally.

While other sets of information security controls may potentially be used within an ISO/IEC 27001 ISMS as well as, or even instead of, ISO/IEC 27002 (the Code of Practice for Information Security Management), these two standards are normally used together in practice. The domains covered by ISO 27002 include:

i. Security policy
ii. Organization of information security
iii. Asset management
iv. Human resources security
v. Physical and environmental security
vi. Communications and operations management
vii. Access control
viii. Information systems acquisition, development and maintenance
ix. Information security incident management
x. Business continuity management
xi. Compliance

Organizations that implement a suite of information security controls in accordance with ISO/IEC 27002 are simultaneously likely to meet many of the requirements of ISO/IEC 27001, but may lack some of the overarching management system elements. The converse is also true, in other words, an ISO/IEC 27001 compliance certificate provides assurance that the management system for information security is in place, but says little about the absolute state of information security within the organization. Technical security controls such as antivirus and firewalls are not normally audited in ISO/IEC 27001 certification audits: the organization is essentially *presumed* to have adopted all necessary information security controls since the overall ISMS is in place and is deemed adequate by satisfying the requirements of ISO/IEC 27001. Furthermore, management determines the scope of the ISMS for certification purposes and may limit it to, say, a single business unit or location. The ISO/IEC 27001 certificate does not necessarily mean the remainder of the organization, outside the scoped area, has an adequate approach to information security management.

Other standards in the ISO/IEC 27000 family of standards provide additional guidance on certain aspects of designing, implementing and operating of ISMS, for example on information security risk management (ISO/IEC 27005).

2.12.2 The PDCA Cycle

The ISO 27001 adopts the process model "Plan-Do-Check-Act" (PDCA) which is applied to the structure of all the processes in ISMS.

Plan (establishing the ISMS): Establish the policy, the ISMS objectives, processes and procedures related to risk management and the improvement of information security to provide results in line with the global policies and objectives of the organization.

Do (implementing and workings of the ISMS): Implement and exploit the ISMS policy, controls, processes and procedures.

Check (monitoring and review of the ISMS): Assess and, if applicable, measure the performances of the processes against the policy, objectives and practical experience and report results to management for review.

Act (update and improvement of the ISMS): Undertake corrective and preventive actions, on the basis of the results of the ISMS internal audit and management review, or other relevant information to continually improve the said system

2.12.3 Origins of ISO/IEC 27001

BS 7799 was a standard originally published by the British Standards Institution (BSI) Group in 1995. It was written by the United Kingdom Government's Department of Trade and Industry (DTI), and consisted of several parts. The first part, containing the best practices for information security management, was revised in 1998; after a lengthy discussion in the worldwide standards bodies, it was eventually adopted by ISO as ISO/IEC 17799, "Information Technology - Code of practice for information security management." in 2000. ISO/IEC 17799 was then revised in June 2005 and finally incorporated in the ISO 27000 series of standards as ISO/IEC 27002 in July 2007.

The second part of BS7799 was first published by BSI in 1999, known as BS 7799 Part 2, titled "Information Security Management Systems - Specification with guidance for use." BS 7799-2 focused on how to implement an Information security management system (ISMS), referring to the information security management structure and controls identified in BS 7799-2. This later became ISO/IEC 27001. The 2002 version of BS 7799-2 introduced the Plan-Do-Check-Act (PDCA) cycle (Deming cycle), aligning it with quality standards such as ISO 9000. BS 7799 Part 2 was adopted by ISO as ISO/IEC 27001 in November 2005. BS 7799 Part 3 was published in 2005, covering risk analysis and management. It aligns with ISO/IEC 27001.

2.12.4 Control objectives and controls

i. Security policy

- *Information security policy:* To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

ii. Organization of information security

- *Internal organization:* To manage information security within the organization.

- *External parties:* To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

iii. Asset management

- *Responsibility for assets:* To achieve and maintain appropriate protection of organizational assets.
- *Information classification:* To ensure that information receives an appropriate level of protection.

iv. Human resources security

- *Prior to employment:* To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.
- *During employment:* To ensure that all employees, contractors and third party users are aware of information security threat sand concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.
- *Termination or change of employment:* To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

v. Physical and environmental security

- *Secure areas:* To prevent unauthorized physical access, damage and interference to the organization's premises and information.
- *Equipment security:* To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

vi. Communications and operations management

- *Operational procedures and responsibilities:* To ensure the correct and secure operation of information processing facilities.
- *Third party service delivery management:* To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

- *System planning and acceptance:* To minimize the risk of systems failures.
- *Protection against malicious and mobile code:* To protect the integrity of software and information.
- *Back-up:* To maintain the integrity and availability of information and information processing facilities.
- *Network security management:* To ensure the protection of information in networks and the protection of the supporting infrastructure.
- *Media handling:* To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.
- *Exchange of information:* To maintain the security of information and software exchanged within an organization and with any external entity.
- *Electronic commerce services:* To ensure the security of electronic commerce services, and their secure use.
- *Monitoring:* To detect unauthorized information processing activities.

vii. Access control

- *Business requirement for access control:* To control access to information.
- *User access management:* To ensure authorized user access and to prevent unauthorized access to information systems.
- *User responsibilities:* To prevent unauthorized user access, and compromise or theft of information and information processing facilities.
- *Network access control:* To prevent unauthorized access to networked services.
- *Operating system access control:* To prevent unauthorized access to operating systems.
- *Application and information access control:* To prevent unauthorized access to information held in application systems.
- *Mobile computing and teleworking:* To ensure information security when using mobile computing and teleworking facilities.

viii. Information systems acquisition, development and maintenance

- *Security requirements of information systems:* To ensure that security is an integral part of information systems.

- *Correct processing in applications:* To prevent errors, loss, unauthorized modification or misuse of information in applications.
- *Cryptographic controls:* To protect the confidentiality, authenticity or integrity of information by cryptographic means.
- *Security of system files:* To ensure the security of system files.
- *Security in development and support processes:* To maintain the security of application system software and information.
- *Technical Vulnerability Management:* To reduce risks resulting from exploitation of published technical vulnerabilities.

ix. Information security incident management

- *Reporting information security events and weaknesses:* To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.
- *Management of information security incidents and improvements:* To ensure a consistent and effective approach is applied to the management of information security incidents.

x. Business continuity management

- *Information security aspects of business continuity management:* To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

xi. Compliance

- *Compliance with legal requirements:* To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.
- *Compliance with security policies and standards, and technical compliance:* To ensure compliance of systems with organizational security policies and standards.
- *Information systems audit considerations:* To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

2.13 Conclusion

This chapter has provided an overview of present-day information security management in the organization. Information security management is essential for effective information security in the organization. However, the present-day approach to information security management in the organization is bureaucratic in nature and technically oriented and, hence, it fails to meet its objectives. The present-day approach, it may be said, actually contributes to the non-compliance of end-users. Hence, if non-compliance is to be remedied, then the present-day approach to information security management too must be enhanced – as stated by (Frangopoulos, 2007), it is improper to use 19th century principles to manage 21st century issues. (Dhillon, 2001a) and (Schlienger & Teufel, 2002) have pointed a way forward towards adopting a *"human-centric"* approach.

CHAPTER (3)
ELECTRONIC MANAGEMEENT

E-management: is the administrative process that is based on the distinct possibilities of the Internet and business networks in the planning, direction and control over the resources and essential capabilities, without limits in order to achieve goals such as: a paperless administration, management without time or many requirements, since it depends on the electronic archive, e-mail, electronic notepads, and voice messages. It is an intelligent network institution relies on knowledge workers (Ghorab, 2003).

3.1 What does e-management mean?

3.2 The concept of e-management

3.3 E-management requirements

3.4 Some e-management techniques

3.5 The basic components of e-management strategy

3.6 E-management significance

- 3.6.1 Importance of e-management concerning organizations
- 3.6.2 Importance of e-management at national level

3.7 The objectives of e- management

3.8 Characteristics of e-management

3.9 Obstacles on transformation towards e-management

3.10 Most important benefits of applying e-management in organizations

3.11 Application of e-management

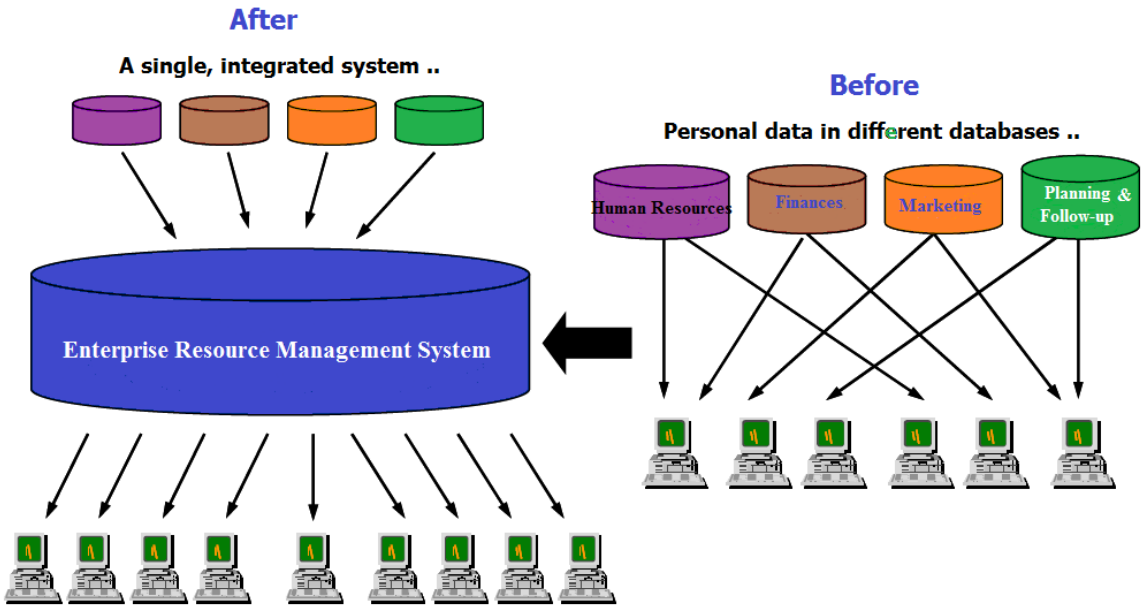
3.12 The potential drawbacks of applying e-management

"Electronic management is the process of mechanizing all assignments and activities belonging to the administrative institution depending on all necessary information techniques for the purpose of fulfilling the new administration objectives in decreasing the use of papers, simplifying procedures, getting rid of routine, reaching accurate and speedy achievements of assignments and transactions. All this is for a final purpose which leads to an administration ready to be related to the electronic government later" (Salmi, 2003).

3.1 What does e-management mean?

The idea of e-management goes far beyond the concept of mechanizing the work within departments of an institution to the concept of integration of data and information between various departments and the use of such data and information to guide the policy and procedures of the institution towards the achievement of its goals, and providing the needed flexibility to respond to successive variables, whether internal or external as shown in Figure (3.1). The electronic management includes all components of the administration: planning, implementation, monitoring, evaluation and stimulating, but it is characterized by its ability to synthesize knowledge continuously and use it for the achievement of objectives. E-management depends on the development of IT infrastructure within the organization to achieve the integration of vision and then perform the work (Al-Kubaisy, 2008).

Figure (3.1): The wider concept of e-management.



3.2 The concept of e-management

The concept of e-management newly emerged as a result of the technical progress and has evolved in the recent years due to the development of information and communication revolution and the increasing demand for the use of computer and its multiple applications. E-management is to perform work and exchange information through electronic means, and this is not only to organizations, but it extends to all segments of society individuals and groups. E-management depends on a range of modern technologies such as the use of computers, networks and e-mail and other electronic means to help in the implementation of business. Thus, we can say that e-management is to transform traditional administrative business to electronic administrative business implemented quickly and accurately. Many features of the contemporary world have contributed to the emergence of this new concept, most notably, single global market, global client and other features. They also have contributed to the movement of the competition from local and regional to global, which has put pressure on an organization to benefit from the modern technology and its new baby (e-management), to provide its services in a way that makes it competitive. This, in turn, create a new trend in the contemporary management of organizations, which converts them into electronic organizations to accomplish their administrative business, such as

planning, organizing, directing and control, quickly to achieve their local, regional and global goals. Thus, e-management has become an indispensable necessity. This study will show some definitions that explain the concept of e-management more clearly (A'l Dahwan, 2008).

Salmi (2003) defines the electronic management as: “the process of mechanizing all assignments and activities belonging to the administrative institution depending on all necessary information techniques for the purpose of fulfilling the new administration objectives in decreasing the use of papers, simplifying procedures, getting rid of routine, reaching accurate and speedy achievements of assignments and transactions. All this is for a final purpose which leads to an administration ready to be related to the electronic government later”. Ghoneim (2004) defines e-management as "the implementation of all business and transactions that take place between two or more parties, whether from individuals or organizations through the use of electronic communications networks", while Najim (2004) defines e-management as "the process which is based on the distinct possibilities of the Internet and business networks in the planning, directing and control over the resources and essential capabilities of the organization, without any limits in order to achieve its goals". Yassin (2005) adds that e-management is "the business systems and activities that are performed electronically and through networks". We note that all the above definitions agree in the fact that the e-management is mechanizing the business, which means transporting and transferring it from paper work to e-business based on the use of modern technology. Given all these definitions, we find that Salmi definition has something of inclusiveness, since he focused on the simplification of procedures, a step that must be done before the process of mechanization, then he mentioned that one of the goals, that every organization will be ready to be linked to the electronic government later, and this refers to the difference between the e-management and the e-government, that the first one precedes the second, and that the electronic management is a first stage, which is made at the level of ministries, agencies, and institutions, e-government comes after that, through the linking process under the so-called electronic gate.

To transform from traditional management to electronic management, it is necessary to achieve the following stages (Al-Kubaisy, 2008):

a) Automate all institutions of the country, and convert all information of the government and its ministries from paper to electronic version.

b) Provide the necessary infrastructure to connect all institutions of the country to a single information network, and exchange information between the various parties.

c) Identify all transactions between the citizen and every institution, and convert them into electronic transactions.

3.3 E-management requirements

Everything which is necessary and required, including moral and material things, so that its availability in the administrative process enables the implementation of business, using modern and safe technological methods that help in the success of e-management programs (A'l Dahwan, 2008).

- Strong networks and communications infrastructure, fast and safe.
- Strong information infrastructure (strong information systems and compatible with each other).
- Electronic means, to take advantage of the services provided by the e-management including personal computers, laptops, phone and other networking devices.
- Quite a number of Internet service providers.
- Human staff capable of investment and trained on the use of modern technologies.
- Human technical staff capable of conducting ongoing technical support and development of various information systems.
- Appropriate level of funding, so that the government can finance periodic maintenance and training of employees, maintain a high level of service delivery and keep up with any development gets under the "e-management" in the world.
- Political will, so that there is an official or a specific committee to implement this project.

- Legislation and legal provisions that facilitate the work of e-management.
- High-level of electronic security and confidentiality, to protect national and personal information and to safeguard the electronic archive of any messes.
- Comprehensive propaganda marketing plan, to promote the use of e-management, highlighting on its features and the need for participation and interaction by all citizens.

In addition to these elements, there must be some technical elements that help to simplify and facilitate the use of e-management commensurate with the culture of all citizens, including: standardization of forms of government and administrative websites and methods used and create a comprehensive guide for addresses of all government and administrative centers in the country (Al-Kubaisy, 2008).

3.4 Some e-management techniques

The following list shows the most famous e-management techniques (Al-Kubaisy, 2008).

- Web Services	- Archiving
- Mobile	- Production Management
- Electronic Document Management	- Performance Assessment
- CRM: Customer Relation Management	- Cooperation of companies programs
- Back office	- . net
- Administrative Intelligence	- Computer Network
- Planning	- Internet

3.5 The basic components of e-management strategy

The four components of the e-management strategy are shown below (Al-Kubaisy, 2008):

IT infrastructure: centralized and safe IT infrastructure, which can be accessed easily by government, private sectors and authorized citizens.

The structure of the legislation and regulations: the structure that supports e-government and e-commerce.

Awareness and learning: the preparation of programs that enhance the efficiency and knowledge of e-government.

Organizational strategy: organizing and coordinating mechanism that helps to implement the e-government strategy.

3.6 E-management significance

The importance of the electronic management will be featured through two axes:

- The first presents its importance at the organizational level.
- The second presents its importance at the national level.

3.6.1 Importance of e-management concerning organizations:

The importance of the e-management is increasingly growing in the light of the information revolution that plays an essential part in administrating changes. It also gained a great significance in deploying knowledge and benefiting of it in fulfilling the organization objectives (A'l Dahwan, 2008).

E-management influences the organization performance at uneven levels, improves work quality and provides assistance to organizations in mastering quick responding to the changes. Moreover, it secures achieving justice, accuracy and transparency when implementing different businesses and transactions (Ghoneim, 2004). Ghonaim (2004) points out to the importance of e-management at the organizational level in providing the help to reduce and limit the dependence on paper-based documents and transactions along with its negative impact. The most outstanding negative effects are presented by wasting time and effort (Ghoneim, 2004).

3.6.2 Importance of e-management at the national level:

E-management provides advantages along with numerous constructive aspects at the national level that all serve the public interest. It also contributes to the growth of the national economy and brings satisfaction to all community categories due to the role it plays in achieving transparency and clarity by which social justice could be fulfilled.

Ghonaim (2004) shows the most significant opportunities can be offered by the e-management as follows:

a) Helps in improving government services to simplify and facilitate procedures and business models and services provided to citizens, and to achieve transparency.

b) Encourages investment in the technical field through the establishment and operation of local industries deal with information technology, and this would contribute to the creation of a national workforce specialized in this field.

c) Provides organizations with an opportunity to be competitive, through what it offers of multiple features, such as saving time and place needed to business performance and reducing the cost of operations.

3.7 The objectives of e- management

- Electronic management seeks to achieve many goals that accrue to the organization a lot of benefits and contribute to the main objective of the organizations, which is raising productivity. Some researchers (Al-Aloul, 2011), (Al-Ajez, 2011) have mentioned some of these goals, which are as follows:
- Managing and following up the various departments of the institution as a central unit.
- Concentrating the decision making point in its own relevant actions and give a greater support to monitor them.
- Collecting data from its original sources uniformly.
- Reducing obstacles of decision-making by providing and linking data.
- Reducing aspects of exchange in the follow-up of the different management operations.
- Deploying IT in order to support and build a positive institute culture for all workers.
- Providing data and information to the beneficiaries immediately.
- Continual learning and knowledge building.

- Increasing interdependence between employees and the higher administration and monitor, and manage all resources (Radwan, 2004).
- Wider distribution of information and make decisions immediately.
- Achieving effective flexibility in the methodology of implementation of activities, and technically and functionally interrelated processes within the organization.
- Getting rid of bureaucratic constraints (Yassin, 2005).
- Contributing to the democratic organization through sharing information, thus removing the regulatory gap between senior management and employees (Najim, 2004).

3.8 Characteristics of e-management

Of the most important characteristics of e-management that it significantly reduces many high-cost things upon which the traditional management used to depend, of which we present here: paper, spatial and temporal borders, too many workers, the magnitude of the buildings and other things that impede the speed and accuracy of performance, (Shawish, 2004) introduces us to the most important characteristics of e-management in the following points:

a) Managing files instead of saving them.
b) Dependence on electronic documents instead of paper in terms of ease of adjustments and speed retrieval.
c) Provide the possibility of attending teleconferences.
d) Providing e-mail as a fast and efficient alternative for incoming and outgoing.
e) Provide electronic follow-up of business being carried out and thus save more time, effort and expenses (Aldafi, 2006).

3.9 Obstacles on transformation towards e-management

Transformation towards e-management needs numerous requirements, either related to the process of organization and management of transformation or to human and material resources. And having weakness or lack in those requirements is a hindrance against transformation, and most important of these obstacles are:

i. Different management systems, even within the same organization.
ii. Having the institute administration not persuaded by the idea of transformation and its requirements
iii. Lack of sound incentive among individuals for working on the success of the transformation process, and lack of belonging to the process of transformation and success.
iv. Difficult access to integrated electronic management within organizations.
v. Lack of good basic technical structure.
vi. Human nature and culture of closed doors and the fear of technology and its applications.
vii. Lack of confidence in the protection of the confidentiality and security of personal transactions (Radwan, 2004).
viii. Lack of computer and information awareness of some administrators who have the decision of adding this technique.
ix. Lack of attention from the side of the senior management in terms of evaluating and following up the application of e-management (Mesfer, 2003).
x. Lack of a proper administrative environment.

3.10 Most important benefits of applying e-management in organizations

E-management has led to a quantum leap in the work of organizations, and is able to achieve a range of benefits, which constitute one of the most important factors to meet the challenges of the contemporary world which marked with the information revolution, and those benefits are as follows (Al-Aloul, 2011), (Al-Ajez, 2011):

- Provide transparency and accountability.
- Encourage initiatives, creativity and innovation.
- Expand information sharing and exchange through modern technical methods.
- Focus on new administrative areas, widening participation in decision-making, and raise awareness of the importance of knowledge and the development of smart capital (Ayoub, 2004).
- Simplification of procedures within institutions and bodies, and its reflection on the level of service provided.

- Shorten the duration of the various administrative transactions.

3.11 Application of e-management

The process of applying e-management is going through two main phases (Al-Aloul, 2011):

First: the stage of creating a work environment that includes re-structuring of work systems, human resources training, and raising awareness among workers about the meaning, importance, and terminology of electronic work.

Second: the stage of providing materials or the technical side of computers, programs, and internal and external networks.

Not going through the first stage or jumping directly to the second weakens the application process and reduces the achievement of e-management objectives. This may expose it to failure, since the e-management is: "The function of completing the work by using systems and electronic means" (Yassin, 2005). This function of the electronic management needs to be preceded by achieving certain regulatory requirements, and "preparing the administrative system to achieve new goals" (Araji & Others, 1982).The Administrative Development Department, in the organization is considered the concerned department to achieve those requirements and to prepare the administrative system, to help the application of e-management as a new target for the organization.

3.12 The potential drawbacks of applying e-management

Some might think that when applying the electronic management strategy, it will go away all the difficulties and the administrative, technical and operational problems, but the actual situation refers to something different, in the sense that the application of electronic management requires an ongoing and sustainable scrutiny to ensure the continued provision of services in the best way with the optimal use of time, money and effort. Taking into account the existence of an alternative plans or emergency plan in case of e-management failed in its work, for whatever possible reasons, and they are generally three main drawbacks (A'l Dahwan, 2008):

a. Electronic spying.
b. Dependency increase.
c. Administrative paralysis.

CHAPTER (4)
RESEARCH METHODOLOGY

4.1 Introduction

This chapter describes the used methodology in this research. It describes the strategy to analyze the impact of information security management on the effectiveness of applying e-management at the Governmental Institutions in Gaza. This chapter will also highlight the research population and the response rate. The chapter includes: research design, data collection resources, research population, pilot study, content validity, questionnaire reliability and the used statistical tests.

4.2 Research Design

The first phase was to develop the research thesis proposal which included identifying and defining the research problem, establishing the study objective and developing the research plan.

The second phase of this research included a summary of a comprehensive literature review. Literatures on information security management and e-management were reviewed.

The third phase included designing the study questionnaire to be used in examining the impact of information security management on the effectiveness of applying e-management at the Governmental Institutions in Gaza.

The fourth phase of this research focused on distributing the questionnaire to a pilot study. The purpose of the pilot study was to test and prove that the questionnaire questions are clear to be answered in a way that will help to achieve the study objectives. Questionnaire validity and reliability tests were conducted for this purpose.

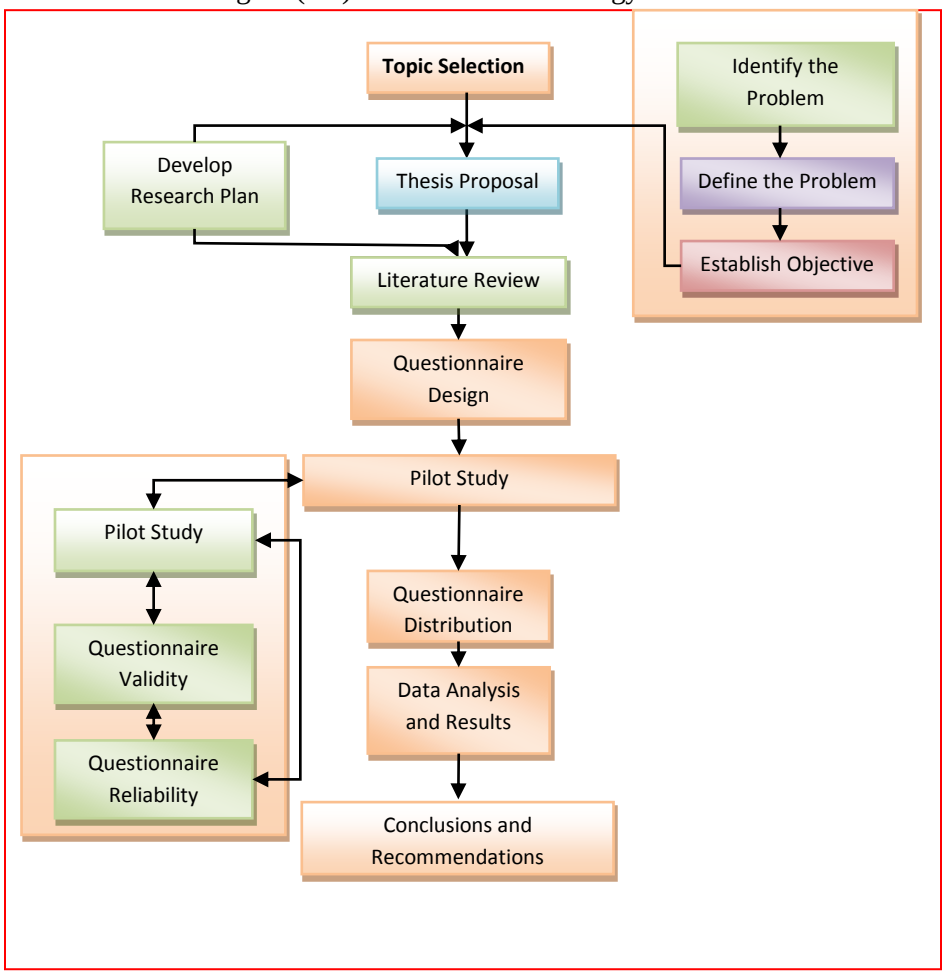
The fifth phase focused on distributing the questionnaire among the study population after ensuring its validity and reliability.

The sixth phase was the data analysis and discussion. Statistical Package for the Social Sciences, (SPSS) was used to perform the required analysis.

The final phase includes the conclusion and recommendations.

Figure (4.1) shows the research methodology flowchart, which leads to achieve its objectives.

Figure (4.1): Research Methodology flow chart.



4.3 Data Collection Resources

In order to achieve the research objectives, two essential data collection resources were used, which are:

1. **Primary Resources:** in order to address the analytical aspects of the research theme, the research resorted to collect the primary data through the questionnaire as a main tool, which is designed especially to meet the research objectives. This questionnaire was distributed among the study population, (158) employees working at the Governmental Institutions in Gaza in order to get their opinions about examining the impact of information security management on the effectiveness of applying e-management at the Governmental Institutions in Gaza.

(8) Governmental Institutions were subjected to the study because they are the only ones that have data centers and apply the e-management in their administrative processes. These Governmental Institutions include: Ministry of Telecommunication and Information Technology, Ministry of Education and Higher Education, Ministry of Health, Ministry of Finance, Ministry of Interior, Ministry of Transportation, Cabinet Secretariat and the General Personnel Council. The targeted employees at these institutions were from the IT and information archiving departments.

2. **Secondary Resources:** in order to address the theoretical background of the study, it has been found on the secondary data collection resources, the likes of books, papers, essays, journals, research studies and reports that have handled the research theme and finally by surfing the internet to the related websites.

4.4 Research Method

This research has used the descriptive analytical approach which tries to describe and evaluate the role of information security management on the effectiveness of applying the e-management at the Governmental Institutions in Gaza. This approach satisfies the research goals in order to compare and evaluate the results, raising our hopes to publicize a meaningful content to support the available knowledge of the research theme.

4.5 Research Population and Sample Size

The population of this study is the Governmental Institutions in Gaza. The research has focused on the staff of information technology, computer based and information archiving departments in those institutions because it discussed the Information Security from a managerial perspective. A comprehensive survey method was used to apply this study on the Governmental Institutions in Gaza, in which this population consists of (158) employees in a variety of job levels working in departments, such as information technology, computer based and information archiving departments. Table (4.1) shows the study population's governmental institution representation.

Table (4.1)
Research Population's Governmental Institution Representation

Governmental Institution	Frequency	Percent (%)
Ministry of Telecommunication and Information Technology	22	13.92
Ministry of Education and Higher Education	14	8.86
Ministry of Health	25	15.82
Ministry of Finance	22	13.92
Ministry of Interior	27	17.09
Ministry of Transportation	9	5.70
Cabinet Secretariat	10	6.33
Personnel Council	29	18.35
Total	158	100.0

Table (4.2) shows the study population's job title representation.

Table (4.2)
Research Population's Job Title Representation

Job Title	Frequency	Percent (%)	Job Title	Frequency	Percent (%)
General Director	6	3.80	Data Entry	14	8.86
Director	18	11.39	Administrative Assistant	23	14.56
Chief Department	30	18.99	Secretary	5	3.16
Chief Branch	2	1.27	Technical	6	3.80
Engineer	29	18.35	Others	4	2.53
Software Developer	21	13.29			
Total	158	100.0			

4.6 Questionnaire Contents

The study questionnaire consists of three parts as the following.

The First Part is a group of the personal characteristics of the respondents and contains (8) questions.

The Second Part is related to the independent variables which actually are the ten fields of information security management. These fields are as the following:

i. **Security Policy:** this field contains (4) items.
ii. **Organizational Security:** this field contains (4) items.
iii. **Asset Classification and Control:** this field contains (4) items.
iv. **Personnel Security:** this field contains (7) items.
v. **Physical and Environmental Security:** this field contains (7) items.
vi. **Computer and Network Management:** this field contains (9) items.
vii. **System Access Control:** this field contains (6) items.
viii. **Systems Development and Maintenance:** this field contains (5) items.
ix. **Business Continuity Planning:** this field contains (4) items.
x. **Compliance to Legal Requirements:** this field contains (4) items.

The Third Part is related to the dependent variable which is the effectiveness of applying the e-management at the Governmental Institutions in Gaza, and contains (15) items.

Thus, the total number of the questions was (69). The respondent can answer the questionnaire item by assigning it with a number from one to ten indicating his/her acceptance degree of this item, where (10) represents the highest acceptance degree about an item and (1) represents the lowest acceptance degree about it.

4.7 Pilot Study

To conduct the pilot study, (30) questionnaires were distributed to an exploratory sample during December, 2012 in order to examine the questionnaire validity and reliability. After ensuring the questionnaire validity and reliability, the researcher had distributed the questionnaire to the residual (128) employees of the population, where

(119) questionnaire were received and five of them were excluded because they were invalid and did not satisfy the required conditions. Thus, the total number of questionnaires subjected to the study and the statistical analysis in the next chapter is (144) questionnaires representing (91.14%) of the study population. The most important characteristics of the study population are explained in the next chapter in detail.

4.8 Questionnaire Validity

We can define the validity of a questionnaire as a determination of the extent to which it actually reflects the abstract construct being examined. Validity refers to the degree to which a questionnaire measures what it is supposed to be measuring. High validity is the absence of systematic errors in the evaluating questionnaire. When a questionnaire is valid; it truly reflects the concept it is supposed to measure.

4.8.1 Arbitrators Validity

Content validity test was conducted by consulting a group of experts. The experts were requested to evaluate and identify whether the questions agreed with the scope of the items and the extent to which these items reflect the concept of the research problem. This group of experts actually were of the academic staff from the Islamic University of Gaza, the Faculty of Commerce, the Faculty of Engineering and Computer Science, the Scientific Research Deanship, other Palestinian Universities and finally from the top management of IT departments in some Governmental Institutions. These arbitrators had issued their suggestions around the questionnaire and its appropriateness to achieve the study objective. In addition, an expert in statistics was requested to evaluate that the used questionnaire is statistically valid and was designed well enough to provide the relations and tests between the study variables. The names and some information about the arbitrators are explained in Appendix (A). The experts did agree that the questionnaire was valid and suitable enough to be used with some amendments. The arbitrators' suggestions and amendments were taken into consideration in order to set the appropriate questionnaire as shown in Appendix (B).

4.8.2 Scale Validity

Consists of the internal validity and the structure validity as what will be explained next. To insure the validity of the questionnaire, two statistical analysis tests

should be applied. The first statistical analysis test is the internal validity test (Pearson Test), which measures the correlation coefficient between each item in the field and the whole field. The second statistical analysis test is the structure validity test (Pearson Test), which used to test the validity of the questionnaire structure and the appropriateness of it to satisfy the study purpose and achieve the research objective by testing the validity of each field and the validity of the whole questionnaire. It measures the correlation coefficient between one filed and all fields of the questionnaire that have the same level of similar scale.

4.8.2.1 Internal Validity (internal consistency)

Internal validity of the questionnaire was evaluated after conducting a pilot study by an exploratory sample, which consisted of thirty questionnaires, by measuring the correlation coefficients between each item in one field and the whole filed. The following tables, from Table (3) through Table (13) show the correlation coefficients and p-values for each field items.

As shown in Table (4.3), the correlation coefficients between each item from the first field "***Security Policy***" and the whole field are located between (0.808) and (0.925) which are high enough to be valid. These correlation coefficients indicate the correlation significance at level ($\alpha = 0.01$) where all p-values are less than (0.01), so it can be said that the items of this field are consistent and valid to measure what they were set for.

Table (4.3)
The correlation coefficient between each item (question) in the field and the whole field
The first field: Security Policy

No.	Item (question)	Pearson correlation coefficient	P-value (sig.)
1	There exists an information security policy known to all the employees.	0.906**	0.000
2	The existed information security policy states the institution approach to manage information security.	0.894**	0.000
3	There is a known and defined responsible department for information security policy and its review, maintenance and upgrade.	0.925**	0.000
4	The maintenance and review process considers any new affecting changes like: significant security incidents, news risks, changes in organizational or technical infrastructure.	0.808**	0.000

** (Indicates Correlation Significance at $\alpha = 0.01$)

As shown in Table (4.4), the correlation coefficients between each item from the second field "***Organizational Security***" and the whole field are located between (0.817) and (0.910) which are high enough to be valid. These correlation coefficients indicate the correlation significance at level ($\alpha = 0.01$) where all p-values are less than (0.01), so it can be said that the items of this field are consistent and valid to measure what they were set for.

Table (4.4)
The correlation coefficient between each item (question) in the field and the whole field
The second field: Organizational Security

No.	Item (question)	Pearson correlation coefficient	P-value (sig.)
1	There is a cross-functional forum of management representatives from relevant parts of the organization to coordinate the implementation of information security controls.	0.846**	0.000
2	Responsibilities for the protection of individual informatics assets and for carrying out specific security processes were clearly defined.	0.910**	0.000
3	Specialized information security advice is obtained where appropriate.	0.856**	0.000
4	The implementation of security policy is reviewed independently on regular basis. This is to provide assurance that organizational practices properly reflect the policy, and that it is feasible and effective.	0.817**	0.000

** (Indicates Correlation Significance at $\alpha = 0.01$)

As shown in Table (4.5), the correlation coefficients between each item from the third field "***Asset Classification and Control***" and the whole field are located between (0.884) and (0.970) which are high enough to be valid. These correlation coefficients indicate the correlation significance at level ($\alpha = 0.01$) where all p-values are less than (0.01), so it can be said that the items of this field are consistent and valid to measure what they were set for.

Table (4.5)
The correlation coefficient between each item (question) in the field and the whole field
The third field: Asset Classification and Control

No.	Item (question)	Pearson correlation coefficient	P-value (sig.)
1	The institution uses a data record file to identify the important assets associated with each information system.	0.884**	0.000
2	There is an Information classification scheme or guideline in place; which will assist in determining how the information is to be handled and protected.	0.970**	0.000
3	An appropriate set of procedures are defined for information labeling and handling in accordance with the classification scheme adopted by the organization.	0.937**	0.000
4	There are existed applied mechanisms enabling the evaluating and controlling the kinds and costs of security incidents and the potential damage.	0.953**	0.000

** (Indicates Correlation Significance at $\alpha = 0.01$)

As shown in Table (4.6), the correlation coefficients between each item from the fourth field "***Personnel Security***" and the whole field are located between (0.719) and (0.836) which are high enough to be valid. These correlation coefficients indicate the correlation significance at level ($\alpha = 0.01$) where all p-values are less than (0.01), so it can be said that the items of this field are consistent and valid to measure what they were set for.

Table (4.6)
The correlation coefficient between each item (question) in the field and the whole field
The fourth field: Personnel Security

No.	Item (question)	Pearson correlation coefficient	P-value (sig.)
1	Security roles and responsibilities as laid in Organization's information security policy are documented in the employee job description card.	0.811**	0.000
2	Employees are asked to sign confidentiality or nondisclosure agreement as a part of their initial terms and conditions of the employment.	0.720**	0.000
3	All employees of the organization receive appropriate Information Security training.	0.810**	0.000
4	Be informed with the staff on the latest updates on the policies and procedures of an organization's information security.	0.810**	0.000
5	A formal reporting procedure exists, to report security incidents through appropriate management channels.	0.814**	0.000
6	A formal reporting procedure or guideline exists for users, to report security weakness in, or threats to, systems or services.	0.836**	0.000
7	There is a formal disciplinary process in place for employees who have violated organizational security policies and procedures.	0.719**	0.000

** (Indicates Correlation Significance at $\alpha = 0.01$)

As shown in Table (4.7), the correlation coefficients between each item from the fifth field "***Physical and Environmental Security***" and the whole field are located between (0.815) and (0.904) which are high enough to be valid. These correlation coefficients indicate the correlation significance at level ($\alpha = 0.01$) where all p-values are less than (0.01), so it can be said that the items of this field are consistent and valid to measure what they were set for.

Table (4.7)
The correlation coefficient between each item (question) in the field and the whole field
The fifth field: Physical and Environmental Security

No.	Item (question)	Pearson correlation coefficient	P-value (sig.)
1	The rooms, which have the Information processing service, are locked or have lockable cabinets or safes.	0.851**	0.000
2	The information is only on need to know basis, which means there exists some security controls for third parties or for personnel working in secure area.	0.893**	0.000
3	The equipment is protected from power failures by using permanence of power supplies such as multiple feeds, UPS, backup generator etc.	0.904**	0.000
4	The power and telecommunication cables carrying data or supporting information services are protected from interception or damage.	0.896**	0.000
5	The equipment is maintained as per the supplier's recommended service intervals and specifications.	0.904**	0.000
6	Disposal storage device containing sensitive information are physically destroyed.	0.815**	0.000
7	Automatic computer screen locking facility is enabled. This would lock the screen when the computer is left unattended for a period.	0.830**	0.000

** (Indicates Correlation Significance at $\alpha = 0.01$)

As shown in Table (4.8), the correlation coefficients between each item from the sixth field "***Computer and Network Management***" and the whole field are located between (0.675) and (0.883) which are high enough to be valid. These correlation coefficients indicate the correlation significance at level ($\alpha = 0.01$) where all p-values are less than (0.01), so it can be said that the items of this field are consistent and valid to measure what they were set for.

Table (4.8)
The correlation coefficient between each item (question) in the field and the whole field
The sixth field: Computer and Network Management

No.	Item (question)	Pearson correlation coefficient	P-value (sig.)
1	The security policy has identified any operating procedures such as back-up, equipment maintenance etc.	0.766**	0.000
2	Audit logs are maintained for any change made to the operating programs.	0.883**	0.000
3	There is existed an Incident Management procedure to handle security incidents.	0.842**	0.000
4	Duties and responsibilities about systems and equipment are separated in order to reduce opportunities for unauthorized modification or misuse of information or services.	0.854**	0.000
5	The capacity demands are monitored and projections of future capacity requirements and equipment upgrades are made.	0.823**	0.000
6	System acceptance criteria are established for new information systems, upgrades and new versions and suitable tests were carried out prior to acceptance.	0.746**	0.000
7	The security policy addresses software licensing issues such as prohibiting usage of unauthorized software.	0.675**	0.000
8	Antivirus software is installed on the computers to check and remove any viruses from computers and media and this software signature is updated regularly.	0.718**	0.000
9	There is a policy in place for the acceptable use of electronic mail.	0.706**	0.000

** (Indicates Correlation Significance at $\alpha = 0.01$)

As shown in Table (4.9), the correlation coefficients between each item from the seventh field "***System Access Control***" and the whole field are located between (0.646) and (0.770) which are high enough to be valid. These correlation coefficients indicate the correlation significance at level ($\alpha = 0.01$) where all p-values are less than (0.01), so it can be said that the items of this field are consistent and valid to measure what they were set for.

Table (4.9)
The correlation coefficient between each item (question) in the field and the whole field
The seventh field: System Access Control

No.	Item (question)	Pearson correlation coefficient	P-value (sig.)
1	The access control policy does address the rules and rights for each user or a group of users.	0.770**	0.000
2	There exists a regular process to review and evaluate user access rights and privileges.	0.748**	0.000
3	There are some guidelines in place to guide users in selecting and maintaining secure passwords.	0.766**	0.000
4	A unique identifier is provided to every user (There are not public accounts used by more than one user).	0.702**	0.000
5	The sensitive systems are provided with isolated computing environment such as running on a dedicated computer, share resources only with trusted application systems.	0.646**	0.000
6	An audit logs recording security relevant events are produced and kept for an agreed period to assist in future investigations and access control monitoring.	0.770**	0.000

** (Indicates Correlation Significance at $\alpha = 0.01$)

As shown in Table (4.10), the correlation coefficients between each item from the eighth field "***Systems Development and Maintenance***" and the whole field are located between (0.717) and (0.910) which are high enough to be valid. These correlation coefficients indicate the correlation significance at level ($\alpha = 0.01$) where all p-values are less than (0.01), so it can be said that the items of this field are consistent and valid to measure what they were set for.

Table (4.10)
The correlation coefficient between each item (question) in the field and the whole field
The eighth field: Systems Development and Maintenance

No.	Item (question)	Pearson correlation coefficient	P-value (sig.)
1	The data input to application system is validated to ensure that it is correct and appropriate.	0.813**	0.000
2	The data output of application system is validated to ensure that the processing of stored information is correct and appropriate.	0.717**	0.000
3	Encryption techniques were used to protect the data.	0.888**	0.000
4	There are some controls in place for the execution of software on operating systems. This is to minimize the risk of corrupting operating systems.	0.885**	0.000
5	There are strict control procedures in place over executing any changes to the information systems to minimize the corruption of them.	0.910**	0.000

** (Indicates Correlation Significance at $\alpha = 0.01$)

As shown in Table (4.11), the correlation coefficients between each item from the ninth field "***Business Continuity Planning***" and the whole field are located between (0.880) and (0.960) which are high enough to be valid. These correlation coefficients indicate the correlation significance at level ($\alpha = 0.01$) where all p-values are less than (0.01), so it can be said that the items of this field are consistent and valid to measure what they were set for.

Table (4.11)
The correlation coefficient between each item (question) in the field and the whole field
The ninth field: Business Continuity Planning

No.	Item (question)	Pearson correlation coefficient	P-value (sig.)
1	There is a managed process in place for developing and maintaining work continuity throughout the organization.	0.880**	0.000
2	The events that could cause interruptions to work process were identified.	0.960**	0.000
3	Plans were developed to restore business operations within the required time frame following an interruption or failure to work process.	0.948**	0.000
4	Work continuity plans are tested regularly to ensure that they are up to date and effective.	0.926**	0.000

** (Indicates Correlation Significance at $\alpha = 0.01$)

As shown in Table (4.12), the correlation coefficients between each item from the tenth field "***Compliance to Legal Requirements***" and the whole field are located between (0.936) and (0.971) which are high enough to be valid. These correlation coefficients indicate the correlation significance at level ($\alpha = 0.01$) where all p-values are less than (0.01), so it can be said that the items of this field are consistent and valid to measure what they were set for.

Table (4.12)
The correlation coefficient between each item (question) in the field and the whole field
The tenth field: Compliance to Legal Requirements

No.	Item (question)	Pearson correlation coefficient	P-value (sig.)
1	All relevant statutory, regulatory and contractual requirements were explicitly defined and documented for each information system.	0.971**	0.000
2	Specific controls and individual responsibilities to meet these requirements were defined and documented.	0.962**	0.000
3	There exist and well implemented some procedures to ensure compliance with legal restrictions on use of material in respect of which there may be intellectual property rights (copyright, design rights, trade marks).	0.936**	0.000
4	All areas within the organization are considered for regular review to ensure compliance with security policy, standards and procedures.	0.939**	0.000

** (Indicates Correlation Significance at $\alpha = 0.01$)

As shown in Table (4.13), the correlation coefficients between each item from the second section "***Effectiveness of Applying e-Management***" and the whole section are located between (0.571) and (0.856) which are high enough to be valid. These correlation coefficients indicate the correlation significance at level ($\alpha = 0.01$) where all p-values are less than (0.01), so it can be said that the items of this section are consistent and valid to measure what they were set for.

Table (4.13)
The correlation coefficient between each item (question) in the field and the whole field
The third part: Effectiveness of applying e-Management

No.	Item (question)	Pearson correlation coefficient	P-value (sig.)
1	The top management supports applying the e-management at the institution.	0.819**	0.000
2	There is a special and appropriate team in place to apply e-management at the institution.	0.808**	0.000
3	The personnel accept the implementation of the e-management at the institution.	0.856**	0.000
4	The personnel have the appropriate knowledge and experience to deal with applying the e-management.	0.682**	0.000
5	The personnel take the needed training on technical tools according to their job needs.	0.670**	0.000
6	The internal administration procedures are done simply without any sophistication.	0.780**	0.000
7	The procedures to serve the out of institution stakeholders are done simply and without any sophistication.	0.803**	0.000
8	There are self-resources in place to ensure the continuity and development of applying the e-management at the strategic term.	0.830**	0.000
9	The institution stakeholders accept to deal with the institution via its internet website.	0.799**	0.000
10	There exist at the institution a lot of the technical requirements like (computers, network, server, hard disks, internet, software and systems).	0.663**	0.000
11	The software applications deliver the sufficient and accurate information properly.	0.794**	0.000
12	The e-management creates a secure environment to exchange information.	0.614**	0.000
13	There exists an effective system to define the authorized users to access the computerized information.	0.619**	0.000
14	The information back-up copies are kept in safe places out the institution.	0.754**	0.000
15	There exist clear and black policies for the personnel who violate the information confidentiality and security.	0.571**	0.000

** (Indicates Correlation Significance at $\alpha = 0.01$)

4.8.2.2 Structure Validity

Structure validity is the second statistical analysis test that was used to evaluate the validity of the questionnaire structure and the appropriateness of it to satisfy the study purpose and to achieve the research objective by testing the validity of each field and the validity of the whole questionnaire. It measures the correlation coefficient between one filed and all fields of the questionnaire that have the same level of a similar scale.

As shown in Table (4.14), the correlation coefficients between each field and the whole questionnaire are located between (0.722) and (0.915) which are high enough to be valid. These correlation coefficients indicate the correlation significance at level (α = 0.01) where all p-values are less than (0.01), so it can be said that the fields of the questionnaire are consistent and valid to measure what they were set for to achieve the study objective.

Table (4.14)
Structure Validity of the Questionnaire

No.	Field	Pearson correlation coefficient	P-value (sig.)
1	Security Policy	0.722**	0.000
2	Organizational Security	0.811**	0.000
3	Asset Classification and Control	0.806**	0.000
4	Personnel Security	0.900**	0.000
5	Physical and Environmental Security	0.846**	0.000
6	Computer and Network Management	0.915**	0.000
7	System Access Control	0.880**	0.000
8	Systems Development and Maintenance	0.834**	0.000
9	Business Continuity Planning	0.825**	0.000
10	Compliance to Legal Requirements	0.836**	0.000
11	Effectiveness of Applying e-Management	0.811**	0.000

** (Indicates Correlation Significance at α = 0.01)

4.9 Questionnaire Reliability

Reliability of a questionnaire is the degree of consistency in which it measures the level of consistency of the questionnaire results if it will be distributed several times under the same conditions. In other words, questionnaire reliability means that the questionnaire will give the same results if it will be distributed several times to the study sample in specific time periods. For the most purposes reliability coefficient above 0.7 is considered satisfactory.

The Cronbach's Alpha statistical test was used to measure the questionnaire reliability. The Alpha values of each field and for all questionnaire items were calculated using Cronbach's Alpha test. As illustrated in Table (4.15), Cronbach's Alpha coefficients are located between (0.821) and (0.965) which are high enough to ensure the reliability of the questionnaire. In addition, the Cronbach's Alpha coefficient for all questionnaire items is (0.983) which also is high to ensure the reliability of the questionnaire.

Table (4.15)
Cronbach's Alpha for Reliability

No.	Field	No. of Items	Cronbach's Alpha coefficient
1	Security Policy	4	0.901
2	Organizational Security	4	0.876
3	Asset Classification and Control	4	0.952
4	Personnel Security	7	0.896
5	Physical and Environmental Security	7	0.945
6	Computer and Network Management	9	0.916
7	System Access Control	6	0.821
8	Systems Development and Maintenance	5	0.898
9	Business Continuity Planning	4	0.943
10	Compliance to Legal Requirements	4	0.965
11	Effectiveness of Applying e-Management	15	0.936
	All Questionnaire Items (questions)	69	0.983

It is clear from the previous analytical results that the questionnaire as shown in Appendix (2) was valid and reliable to pursue distributing it among the study sample and to rely on it in answering the study questions and analyzing its hypothesis.

4.10 Statistical Methods

The Statistical Package for Social Science (SPSS) software was used to analyze this research data. The following statistical tests were used to analyze the data and the study hypothesis:

i. Frequencies, means and percentages to represent the collected data in meaningful figures.
ii. Pearson Correlation Coefficient was used to measure the correlation between two variables, where it was applied to test the questionnaire validity.
iii. Cronbach's Alpha coefficient was used to test the questionnaire reliability.
iv. One Sample Kolmogorov-Smirnov test was used to identify if the study questionnaire data follows the normal distribution or not, this test is considered necessary in the case of testing hypotheses as most Parametric Tests stipulate data to be normally distributed.
v. The One-Sample T test was used to determine the statistical mean of each item (question) in the questionnaire field and compare it with the neutrality degree of (6). This test was used to answer the study questions.
vi. The Pearson Correlation Coefficient test was used to examine the correlation significance in testing the first main hypothesis.
vii. The Two-independent samples T Test was used to determine if there are differences indicating statistical significance between the means of two groups of data like the respondents' gender (male and female).
viii. The One-Way ANOVA test was used to determine if there are differences indicating statistical significance between the means in the case of three groups of data and more like the respondents' qualification (general secondary, diploma, bachelor and master).

CHAPTER (5)
DATA ANALYSIS AND DISCUSSION

5.1 Introduction:

This chapter highlights the statistical techniques were used in analyzing this research data and finding out the appropriate answers to the study questions. In addition, this chapter describes the used techniques in testing the research hypothesis. This chapter also highlights the characteristics of research population.

5.2 Normality Distribution Test

One Sample Kolmogorov-Smirnov test was used to identify if the study questionnaire data follows the normal distribution or not, this test is considered necessary in the case of testing hypotheses as most Parametric Tests stipulate data to be normally distributed.

Table (5.1)
One Sample Kolmogorov-Smirnov Test

No.	Field	No. of Items	P-value (sig.)
1	Information Security Managements Fields	54	0.200
2	Effectiveness of Applying e-Management Field	15	0.056
3	All Fields of the Questionnaire	69	0.200

Table (5.1) clarifies that the calculated sig. (p-values) for the questionnaire fields were greater than the significance level at ($\alpha = 0.05$), (p-value > 0.05). This in turn indicated that the study data followed the normal distribution, and so the Parametric Tests were used in analyzing the study hypothesis and finding the appropriate answers for its questions.

5.3 Data Analysis:

5.3.1 Sample Characteristics:

This section introduces the descriptive statistics of the study respondents' characteristics (sample characteristics). These sample characteristics include: their gender, qualification, specialty, age, job title, experience and the governmental institution they belong to. This descriptive statistical analysis was done using the available data in the first part of the study questionnaire as illustrated in Appendix (B).

5.3.1.1 Respondents' Gender:

Table (5.2)
Respondents' Gender Representation

Gender	Frequency	Percent (%)
Male	114	79.2
Female	30	20.8
Total	144	100.0

Table (5.2) illustrates that (79.2%) of the respondents are male, while (20.8%) of them are female. It is clear from this result that the males' proportion is greater than the females' one. This reflects the limitation of women participation among the work force. This ratio approaches the work force structure in Palestine in 2010 which amounts to (82%) males and (18%) females (Palestinian Central Bureau of Statistics, 2011).

5.3.1.2 Respondents' Level of Qualification:

Table (5.3)
Respondents' Level of Qualification Representation

Level of Qualification	Frequency	Percent (%)
General Secondary and below	4	2.8
Diploma	17	11.8
Bachelor	113	78.5
Master	10	6.9
Total	144	100.0

Table (5.3) illustrates that (78.5%) of the respondents are having the bachelor degree, and (11.8%) of them are having the diploma degree, and (6.9%) of them are having the master degree, while (2.8%) of them are having the general secondary degree or below. From the concluded result, it is clear that most of the respondents are well educated and having the bachelor and master degrees. This result could be attributed to the minimum qualification requirements that are needed to be hired in information technology jobs as they set by the General Personnel Council and this reflects the government interest in choosing its employees. This result is greater than what Ammar (2009) has concluded that (70.8%) were having the bachelor degree in his study about the

available requirements to apply e-management in UNRWA, and less than what Al-Ghoty (2006) has concluded that (96.6%) were having the bachelor degree in his study about the available requirements to apply e-Government in Gaza.

5.3.1.3 Respondents' Specialization:

Table (5.4)
Respondents' Specialization Representation

Specialty	Frequency	Percent (%)
Computer Engineering	55	38.2
Computer Science	22	15.3
Information Technology	18	12.5
Business Administration	18	12.5
Electricity and Communication Engineer	4	2.8
Others	27	18.8
Total	144	100.0

Table (5.4) illustrates that (38.2%) of the respondents are computer engineers, and (27.8%) of them are software developers, while (12.5%) of them are having the business administration certificate. This clarifies the diversity of specialization among the work force and it could be noticed the majority of computer engineers. This result could be attributed to the government attempt to enhance the IT units in order to achieve remarkable steps towards the successful launch of e-Government.

5.3.1.4 Respondents' Age:

Table (5.5)
Respondents' Age Representation

Age	Frequency	Percent (%)
Less than 30	78	54.2
30 to less than 40	53	36.8
40 to less than 50	12	8.3
50 and older	1	0.7
Total	144	100.0

Table (5.5) illustrates that (54.2%) of the respondents are less than (30) years old and (45.1%) of them are between (30) to (50) years old. This reflects the youth participation among the work force and it could be concluded that the IT body is youth and capable to exert the best in its career. This result could be attributed to the fact that IT generation is relatively new and becomes an essential part of our contemporary life.

5.3.1.5 Respondents' Job Title:

Table (5.6)
Respondents' Job Title Representation

Job Title	Frequency	Percent (%)	Job Title	Frequency	Percent (%)
General Director	6	4.2	Data Entry	12	8.3
Director	17	11.8	Administrative Assistant	22	15.3
Chief Department	28	19.4	Secretary	4	2.8
Chief Branch	1	0.7	Technical	5	3.5
Engineer	26	18.1	Others	4	2.8
Software Developer	19	13.2			
Total	144	100.0			

Table (5.6) illustrates that (4.2%) of the respondents are General Directors, and (11.8%) of them are Directors, and (19.4%) of them are Chiefs of Departments, and (18.1%) of them are Engineers, and (13.2%) of them are Software Developers, while (15.3%) of them are Administrative Assistants. This reflects the diversity of job titles among the respondents.

5.3.1.6 Respondents' Experience:

Table (5.7)
Respondents' Experience Representation

Experience	Frequency	Percent (%)
Less than 4 years	61	42.4
4 years to less than 8 years	58	40.3
8 years to less than 12 years	8	5.6
12 years to less than 16 years	10	6.9
16 years and more	7	4.9
Total	144	100.0

Table (5.7) illustrates that (42.4%) of the respondents have experience less than (4) years, and (40.3%) of them have experience between (4) and (8) years while (17.4%) of them have experience more than (8) years. This clarifies that about half of the respondents have experience less than (4) years. This result could be attributed to the government efforts to fill the available vacancies after the Palestinian division events.

5.3.1.7 Respondents' Governmental Institution:

Table (5.8)
Respondents' Governmental Institution Representation

Governmental Institution	Frequency	Percent (%)
Ministry of Telecommunication and Information Technology	18	12.5
Ministry of Education and Higher Education	13	9.0
Ministry of Health	18	12.5
Ministry of Finance	22	15.3
Ministry of Interior	27	18.8
Ministry of Transportation	7	4.9
Cabinet Secretariat	10	6.9
Personnel Council	29	20.1
Total	144	100.0

Table (5.8) illustrates that (20.1%) of the respondents are from the General Personnel Council, and (18.8%) of them are from the Ministry of Interior, and (15.3%) of them are from the Ministry of Finance, and (12.5%) of them are from the Ministry of Telecommunication and Information Technology, and (12.5%) of them are from the Ministry of Health, and (9%) of them are from the Ministry of Education and Higher Education, and (6.9%) of them are from the Cabinet Secretariat, while (4.9%) of them are from the Ministry of Transportation. This result reflects the higher number of staff and response rate of the ministries like: Ministry of Finance, Ministry of Interior, and the General Personnel Council.

5.3.2 Study Fields Analysis

In order to answer the study questions, the research used One-Sample T test in analyzing the questionnaire fields related to the study questions. One-Sample T test was used to determine the statistical mean of each item (question) in the field and compare it with the neutrality degree of (6). The result of this test determined if the response to an item of the questionnaire fields was equal to the neutrality degree of (6) or differed than it significantly.

Null Hypothesis: The tested item response mean is equal to (6) which is corresponding to the chosen neutrality degree on the used scale to answer the questionnaire items which is from (1) indicating the minimum degree of acceptance on the item content through (10) indicating the maximum degree of acceptance on the item content. This could be confirmed if the sig. (p-value) was greater than the significance level at ($\alpha = 0.05$) this implies that the response mean of the study sample approached the neutrality degree of (6). This result corresponds to accept the null hypothesis and reject the alternative one.

Alternative Hypothesis: The tested item response mean differs than (6) which is the chosen neutrality degree on the used scale to answer the questionnaire items. This could be confirmed if the sig. (p-value) was less than or equaled the significance level at ($\alpha = 0.05$), this implies that the response mean of the study sample differed significantly than the neutrality degree of (6). This result corresponds to reject the null hypothesis and accept the alternative one. In this case, the sign of One-Sample T test value determined whether the response mean was greater or less than the neutrality degree of (6) significantly. If the sign of One-Sample T test value was positive, this revealed that the response mean was greater than the neutrality degree of (6) and the opposite is correct.

The items (questions) of each field in the questionnaire were ranked in descending order according to the acceptance degree, where the rank (1) represents the item that has the highest acceptance degree.

5.3.2.1 Analysis of Information Security Management Fields

Tables (5.9) to (5.19) illustrate the results of using One-Sample T test in analyzing each item in the fields of information security management.

5.3.2.1.1 Field One: Security Policy

Table (5.9)
One-Sample T test mean and P-value (sig.) of the first field: Security Policy

No.	Item (question)	Mean	Weight Mean	P-value (sig.)	Test Value (T)	Order
1	There exists an information security policy known to all the employees.	6.14	61.40	0.418	.811	4
2	The existed information security policy states the organization approach to manage information security.	6.37	63.70	0.033	2.150	3
3	There is a known and defined responsible department for information security policy and its review, maintenance and upgrade.	7.27	72.70	0.000	6.125	1
4	The maintenance and review process considers any new affecting changes like: significant security incidents, news risks, changes in organizational or technical infrastructure.	6.72	67.20	0.000	4.120	2
All the items of the field		6.63	66.30	0.000	4.167	

(Statistical Significance at level $\alpha = 0.05$)

Table (5.9) shows the respondents' opinions towards the items of the first field "***Security Policy***" as they are ranked in a descending order according to the acceptance degree, where the rank (1) represents the item that has the highest acceptance degree. The following facts could be concluded:

- The statistical mean for item (3) equals (7.27), the weight mean equals (72.70%) and the sig. (p-value) equals (0.000), which shows statistical significance and that the response level of this item is greater than the neutrality degree of (6). This implies that the respondents agree that "*There is a known and defined responsible department for information security policy and its review, maintenance and upgrade*". This result partially agrees with what Tayeh (2008) has found in his study about the effectiveness of information security management in the Palestinian IT companies. This fact could be attributed to the government attention to enhance

the information security departments. The finding also agrees with Al-Otaibi (2010) in his study about the information security of websites and its compatibility with local and international standards, as he found a compatibility degree of the information security strategies with local and international standards.

- The statistical mean for item (1) equals (6.14), the weight mean equals (61.40%) and the sig. (p-value) equals (0.418) greater than ($\alpha = 0.05$), which does not show statistical significance and reveals that the response mean of this item does not differ significantly than the neutrality degree of (6). This result does not agree with Tayeh (2008) that has shown the respondents' acceptance of this item. This fact requires the government to pay more attention to enhance the employee awareness of information security and exert more efforts to establish information security policies known to all employees.
- In general, the statistical mean for the whole field "*Security Policy*" equals (6.63), the weight mean equals (66.30%) and the sig. (p-value) equals (0.000) less than ($\alpha = 0.05$), which shows statistical significance and that the response level of this field is greater than the neutrality degree of (6). This indicates that the respondents agree with the field "*Security Policy*". This result agrees with Yildirim, Akalp, Aytac, & Bayram (2011) that said when security policy improve other security parameters in the companies, such as Organizational, Personnel and Physical and Environmental Securities improve as well. The finding also agrees with Tayeh (2008) which stated that there is a significant effect of information security policy on the effectiveness of information security management in the Palestinian IT companies. This result also agrees with the study of Knapp & others (2006) which stated that the top management support is a key factor of the organization's security culture and level of policy enforcement.

5.3.2.1.2 Field Two: Organizational Security

Table (5.10)
One-Sample T test mean and P-value (sig.) of the second field: Organizational Security

No.	Item (question)	Mean	Weight Mean	P-value (sig.)	Test Value (T)	Order
1	There is a cross-functional forum of management representatives from relevant parts of the organization to coordinate the implementation of information security controls.	5.99	59.90	0.977	-.028	2
2	Responsibilities for the protection of individual informatics assets and for carrying out specific security processes were clearly defined.	6.31	63.10	0.102	1.647	1
3	Specialized information security advice is obtained where appropriate.	5.30	53.00	0.002	-3.221	3
4	The implementation of security policy is reviewed independently on regular basis. This is to provide assurance that organizational practices properly reflect the policy, and that it is feasible and effective.	4.40	44.0	0.000	-7.451	4
All the items of the field		5.60	56.00	0.004	-2.891	

(Statistical Significance at level $\alpha = 0.05$)

Table (5.10) shows the respondents' opinions towards the items of the second field "***Organizational Security***". The following facts could be concluded:

- The statistical mean for item (2) equals (6.31), the weight mean equals (63.10%) and the sig. (p-value) equals (0.102) greater than ($\alpha = 0.05$), which does not show statistical significance and that the response level of this item does not differ significantly than the neutrality degree of (6). This result agrees with what Tayeh (2008) has found in his study about the effectiveness of information security management in the Palestinian IT companies.
- The statistical mean for item (4) equals (4.40), the weight mean equals (44.00%) and the sig. (p-value) equals (0.000) less than ($\alpha = 0.05$), which shows statistical significance and that the response level of this item is less than the neutrality degree of (6). This indicates that the respondents disagree with "*The implementation of security policy is reviewed independently on regular basis. This is to provide assurance that organizational practices properly reflect the policy, and that it is*

feasible and effective". The finding agrees with Hong K. , Chi, Chao, & Tang (2003) that studied an integrated system theory of information security management and found a proposed theory that provides rich information security strategies, procedures and theories for researchers, information security decision makers, planners, providers and users; thereby they can get a better understanding of information security in terms of different perspectives. This result also agrees with what Tayeh (2008) has found in his study about the effectiveness of information security management in the Palestinian IT companies, where the response weight mean of this item equals (45.12%). This fact requires the government to pay more attention to enhance reviewing the implementation of security policy regularly.

- In general, the statistical mean for the whole field "*Organizational Security*" equals (5.60), the weight mean equals (56.00%) and the sig. (p-value) equals (0.004) less than ($\alpha = 0.05$), which shows statistical significance and that the response level of this field is less than the neutrality degree of (6). This indicates that the respondents disagree with the field "*Organizational Security*". This result agrees with the study of Tayeh (2008) where he has found the response weight of the effect of the organizational security on the effectiveness of information security management in the Palestinian IT companies equals (55.64%). This result could be referred to the lack of involving employees and considering them as a major part in the security management process. This also agrees with Belsis and Kokolakis (2005) who argued that most stakeholders lack the required knowledge of Information Systems (IS) security issues that would allow them to play an important role in IS security management.

5.3.2.1.3 Field Three: Asset Classification and Control

Table (5.11)
One-Sample T test mean and P-value (sig.) of the third field: Asset Classification and Control

No.	Item (question)	Mean	Weight Mean	P-value (sig.)	Test Value (T)	Order
1	The organization uses a data record file to identify the important assets associated with each information system.	7.05	70.50	0.000	5.669	1
2	There is an Information classification scheme or guideline in place; which will assist in determining how the information is to be handled and protected.	5.69	56.90	0.158	-1.419	3
3	An appropriate set of procedures are defined for information labeling and handling in accordance with the classification scheme adopted by the organization.	5.81	58.10	0.370	-.900	2
4	There are existed applied mechanisms enabling the evaluating and controlling the kinds and costs of security incidents and the potential damage.	5.44	54.40	0.007	-2.742	4
All the items of the field		6.00	60.00	1.000	.000	

(Statistical Significance at level $\alpha = 0.05$)

Table (5.11) shows the respondents' opinions towards the items of the third field "***Asset Classification and Control***". The following facts could be concluded:

- The statistical mean for item (1) equals (7.05), the weight mean equals (70.50%) and the sig. (p-value) equals (0.000) less than ($\alpha = 0.05$), which shows statistical significance and shows that the response level of this item is greater than the neutrality degree of (6). This indicates that the respondents agree that "*The organization uses a data record file to identify the important assets associated with each information system*". This result agrees with what Tayeh (2008) has found in his study about the effectiveness of information security management in the Palestinian IT companies, where the response weight mean equaled (%77.44) over this item. This fact could be attributed to the government attention to enhance the procedures of asset classification.
- The statistical mean for item (4) equals (5.44), the weight mean equals (54.40%) and the sig. (p-value) equals (0.007) less than ($\alpha = 0.05$), which shows statistical significance and that the response level of this item is less than the neutrality

degree of (6). This reveals that the respondents disagree with "*There are existed applied mechanisms enabling the evaluating and controlling the kinds and costs of security incidents and the potential damage*". The finding agrees with Hong K. , Chi, Chao, & Tang (2003) that studied an integrated system theory of information security management and found a proposed theory that could be a building block for further information security management researchers and be a guidance of future empirical studies. This result does not agree with what Tayeh (2008) has found in his study about the effectiveness of information security management in the Palestinian IT companies, where the response weight mean equaled (%71.34) over this item. From this result, it is obvious that the government is required to enhance the needed mechanisms to evaluate and control the potential incidents and damage.

- In general, the statistical mean for the whole field "*Asset Classification and Control*" equals (6.00), the weight mean equals (60.00%) and the sig. (p-value) equals (1.000) greater than ($\alpha = 0.05$), which definitely shows that the response level of this field equals the neutrality degree of (6). This implies that the respondents did not formulate a clear satisfaction about the field "*Asset Classification and Control*". This result disagrees with the study Tayeh (2008) where he has found the response weight of the effect of the Asset Classification and Control on the effectiveness of information security management in the Palestinian IT companies equaled (72.97%). This fact requires the government to exert more efforts in asset classification and handle the appropriate labeling procedures considering them as a major part in the security management process. This also agrees with Fiedler (2003) who stated that it is important for organizations to have an inventory of all information assets given in an organization in order to protect their information assets. The author also added that a classification of information assets helps to characterize these assets and assign appropriate protective actions.

5.3.2.1.4 Field Four: Personnel Security

Table (5.12)
One-Sample T test mean and P-value (sig.) of the fourth field: Personnel Security

No.	Item (question)	Mean	Weight Mean	P-value (sig.)	Test Value (T)	Order
1	Security roles and responsibilities as laid in Organization's information security policy are documented in the employee job description card.	5.51	55.10	0.028	-2.220	3
2	Employees are asked to sign confidentiality or nondisclosure agreement as a part of their initial terms and conditions of the employment.	6.20	62.00	0.446	.764	1
3	All employees of the organization receive appropriate Information Security training.	4.42	44.20	0.000	-7.664	7
4	Be informed with the staff on the latest updates on the policies and procedures of an organization's information security.	4.75	47.50	0.000	-5.625	6
5	A formal reporting procedure exists, to report security incidents through appropriate management channels.	5.42	54.20	0.006	-2.814	4
6	A formal reporting procedure or guideline exists for users, to report security weakness in, or threats to, systems or services.	5.02	50.20	0.000	-4.756	5
7	There is a formal disciplinary process in place for employees who have violated organizational security policies and procedures.	6.06	60.60	0.777	.284	2
All the items of the field		5.34	53.40	0.000	-3.956	

(Statistical Significance at level $\alpha = 0.05$)

Table (5.12) shows the respondents' opinions towards the items of the fourth field "***Personnel Security***". The following facts could be concluded:

- The statistical mean for item (2) equals (6.20), the weight mean equals (62.00%) and the sig. (p-value) equals (0.446) greater than ($\alpha = 0.05$), which does not show statistical significance and reveals that the response level of this item does not differ significantly than the neutrality degree of (6). The finding agrees with Hong K. , Chi, Chao, & Tang (2003) that studied an integrated system theory of information security management and found a proposed theory that explains

organizational behavior regarding information security management, and provides alternatives for organizational security management strategies. This result also agrees with what Tayeh (2008) has found in his study about the effectiveness of information security management in the Palestinian IT companies as the response weight mean equaled (%68.29) over this item. This fact requires the government to exert more efforts in order to ensure the personnel security.

- The statistical mean for item (3) equals (4.42), the weight mean equals (44.20%) and the sig. (p-value) equals (0.000) less than ($\alpha = 0.05$), which shows statistical significance and that the response level of this item is less than the neutrality degree of (6). This indicates that the respondents do not agree with "*All employees of the organization receive appropriate Information Security training*". This result do not agree with what Tayeh (2008) has found in his study about the effectiveness of information security management at the Palestinian IT companies, where the response weight mean equaled (%56.10) over this item. This reflects the lack of training the personnel on information security. From this result, it is obvious that the government is required to enhance the needed training programs on information security for its staff.
- In general, the statistical mean for the whole field "*Personnel Security*" equals (5.34), the weight mean equals (53.40%) and the sig. (p-value) equals (0.000) less than ($\alpha = 0.05$), which shows that the response level of this field is less than the neutrality degree of (6). This indicates that the respondents do not agree with the field "*Personnel Security*". This result partially agrees with the study of Tayeh (2008) where he has found the response weight of the effect of personnel security field on the effectiveness of information security management in the Palestinian IT companies equaled (60.54%). This fact requires the government to exert more efforts in enhancing the personnel security by proceeding effective staff training on information security and formal reporting about the weaknesses. This also agrees with the results of the 2006 Australian Computer Crime and Security Survey (AHTCC, AFP, & Others, 2006) that conducted by The Australian High Tech Crime Centre (AHTCC), the Australian Federal Police (AFP) and many

other organizations, which show that (62%) of respondents experiencing insider abuse of Internet access, email or computer system resources.

5.3.2.1.5 Field Five: Physical and Environmental Security

Table (5.13)
One-Sample T test mean and P-value (sig.) of the fifth field: Physical and Environmental Security

No.	Item (question)	Mean	Weight Mean	P-value (sig.)	Test Value (T)	Order
1	The rooms, which have the Information processing service, are locked or have lockable cabinets or safes.	7.49	74.90	0.000	7.844	3
2	The information is only on need to know basis, which means there exists some security controls for third parties or for personnel working in secure area.	7.68	76.80	0.000	10.858	2
3	The equipment is protected from power failures by using permanence power supplies such as multiple feeds, UPS, backup generator etc.	7.88	78.80	0.000	9.673	1
4	The power and telecommunication cables carrying data or supporting information services are protected from interception or damage.	7.43	74.30	0.000	8.759	4
5	The equipment is maintained as per the supplier's recommended service intervals and specifications.	7.03	70.30	0.000	6.078	5
6	Disposal storage device containing sensitive information are physically destroyed.	6.65	66.50	0.001	3.541	7
7	Automatic computer screen locking facility is enabled. This would lock the screen when the computer is left unattended for a period.	7.01	70.10	0.000	5.571	6
All the items of the field		7.31	73.10	0.000	9.907	

(Statistical Significance at level $\alpha = 0.05$)

Table (5.13) shows the respondents' opinions towards the items of the fifth field "***Physical and Environmental Security***". The following facts could be concluded:

- The statistical mean for item (3) equals (7.88), the weight mean equals (78.80%) and the sig. (p-value) equals (0.000) less than ($\alpha = 0.05$), which shows statistical significance and that the response level of this item is greater than the neutrality degree of (6). This indicates that the respondents agree with "*The equipment is*

protected from power failures by using permanence power supplies such as multiple feeds, UPS, backup generator etc." This result agrees with what Tayeh (2008) has found in his study about the effectiveness of information security management in the Palestinian IT companies, where the response weight mean equaled (%81.71) over this item. This fact could be attributed to the government attention to preserve equipment from failures especially because of the sophisticated nature of the power supply in Gaza.

- The statistical mean for item (6) equals (6.65), the weight mean equals (66.50%) and the sig. (p-value) equals (0.001) less than ($\alpha = 0.05$), which shows statistical significance and that the response level of this item is greater than the neutrality degree of (6). This implies that the respondents moderately agree that "*Disposal storage device containing sensitive information are physically destroyed*". This result agrees with what Tayeh (2008) has found in his study about the effectiveness of information security management in the Palestinian IT companies, where the response weight mean equaled (%77.44) over this item. This fact could be attributed to the well awareness among the government responsible staff in the disposal process of the no longer needed storage devices.
- In general, the statistical mean for the whole field "*Physical and Environmental Security*" equals (7.31), the weight mean equals (73.10%) and the sig. (p-value) equals (0.000) less than ($\alpha = 0.05$), which shows that the response level of this field is greater than the neutrality degree of (6). This indicates that the respondents agree with the field "*Physical and Environmental Security*". This result agrees with the study of Tayeh (2008) where he has found the response weight of the effect of the physical and environmental security on the effectiveness of information security management in the Palestinian IT companies equals (77.89%). This fact requires the government to exert more efforts in enhancing the physical and environmental security by proceeding effective preserving measures for the equipment from the potential security risks. This also agrees with Steinkea (2011) who stated that if the physical integrity of one computer in an organization is compromised, information security could be at risk. The author also added that if someone were to gain unauthorized physical access to a

computer, he/she could also gain access to all of the information on that computer and possibly any other resource that computer is connected to.

5.3.2.1.6 Field Six: Computer and Network Management

Table (5.14)
One-Sample T test mean and P-value (sig.) of the sixth field: Computer and Network Management

No.	Item (question)	Mean	Weight Mean	P-value (sig.)	Test Value (T)	Order
1	The security policy has identified any operating procedures such as back-up, equipment maintenance etc.	7.95	79.50	0.000	13.401	1
2	Audit logs are maintained for any change made to the operating programs.	6.84	68.40	0.000	4.599	7
3	There is existed an Incident Management procedure to handle security incidents.	6.21	62.10	0.214	1.248	8
4	Duties and responsibilities about systems and equipment are separated in order to reduce opportunities for unauthorized modification or misuse of information or services.	7.03	70.30	0.000	6.433	4
5	The capacity demands are monitored and projections of future capacity requirements and equipment upgrades are made.	7.00	70.00	0.000	6.000	5
6	System acceptance criteria are established for new information systems, upgrades and new versions and suitable tests were carried out prior to acceptance.	7.12	71.20	0.000	6.936	3
7	The security policy addresses software licensing issues such as prohibiting usage of unauthorized software.	5.57	55.70	0.048	-1.993	9
8	Antivirus software is installed on the computers to check and remove any viruses from computers and media and this software signature is updated regularly.	7.72	77.20	0.000	10.907	2
9	There is a policy in place for the acceptable use of electronic mail.	6.93	69.30	0.000	5.577	6
All the items of the field		6.93	69.30	0.000	7.941	

(Statistical Significance at level $\alpha = 0.05$)

Table (5.14) shows the respondents' opinions towards the items of the sixth field "***Computer and Network Management***". The following facts could be concluded:

- The statistical mean for item (1) equals (7.95), the weight mean equals (79.50%) and the sig. (p-value) equals (0.000), less than (α = 0.05), which shows statistical significance and that the response level of this item is greater than the neutrality degree of (6). This implies that the respondents agree that "*The security policy has identified any operating procedures such as back-up, equipment maintenance etc.*" This finding agrees with Lee & Lee (2002) in their study a holistic model of computer abuse within organizations as the authors concluded that the new model contributes to the theoretical body of knowledge on computer abuse by providing a new angle for approaching the problem, and it suggests to practitioners that both technical and social solutions should be implemented to reduce the pervasive computer abuse problems. This result agrees with what Tayeh (2008) has found in his study about the effectiveness of information security management in the Palestinian IT companies, where the response weight mean equaled (%82.93) over this item. This fact could be attributed to the government attention in applying operating procedures compatible with the security policy.
- The statistical mean for item (7) equals (5.57), the weight mean equals (55.70%) and the sig. (p-value) equals (0.048), less than (α = 0.05), which shows statistical significance and that the response level of this item is less than the neutrality degree of (6). This indicates that the respondents disagree that "*The security policy addresses software licensing issues such as prohibiting usage of unauthorized software*". This result agrees with what Tayeh (2008) has found in his study about the effectiveness of information security management in the Palestinian IT companies, where the response weight mean equaled (%56.71) over this item. This fact could be attributed to the absence of the needed legislation related to software intellectual property rights, hence, it is required that the government should organize and issue the needed legislation and roles to regulate the software intellectual property rights.
- In general, the statistical mean for the whole field "*Computer and Network Management*" equals (6.93), the weight mean equals (69.30%) and the sig. (p-value) equals (0.000) less than (α = 0.05), which shows that the response level of this field is greater than the neutrality degree of (6). This reveals that the

respondents agree with the field "*Computer and Network Management*". The finding agrees with Chan & Kwok (2001) in their study, integrating security design into the software development process for e-commerce systems as the authors proposed a software development process for secured systems (SDPSS) based on unified modeling language (UML), in which security design is integrated and means are provided to check whether the security requirements have been incorporated into the final design. This result also agrees with the study of Tayeh (2008) where he has found the response weight of the effect of the computer and network management on the effectiveness of information security management at the Palestinian IT companies equals (75.32%). This fact requires the government to exert more efforts in enhancing the computer and network management by proceeding effective operating procedures and ensuring the avoidance of potential security risks.

5.3.2.1.7 Field Seven: System Access Control

Table (5.15)
One-Sample T test mean and P-value (sig.) of the seventh field: System Access Control

No.	Item (question)	Mean	Weight Mean	P-value (sig.)	Test Value (T)	Order
1	The access control policy does address the rules and rights for each user or a group of users.	7.78	77.80	0.000	11.590	2
2	There exists a regular process to review and evaluate user access rights and privileges.	6.97	69.70	0.000	5.839	5
3	There are some guidelines in place to guide users in selecting and maintaining secure passwords.	6.69	66.90	0.000	3.786	6
4	A unique identifier is provided to every user (There are not public accounts used by more than one user).	8.57	85.70	0.000	19.785	1
5	The sensitive systems are provided with isolated computing environment such as running on a dedicated computer, share resources only with trusted application systems.	7.73	77.30	0.000	11.440	3
6	An audit logs recording security relevant events are produced and kept for an agreed period to assist in future investigations and access control monitoring.	7.07	70.70	0.000	5.730	4
All the items of the field		7.47	74.70	0.000	12.730	

(Statistical Significance at level $\alpha = 0.05$)

Table (5.15) shows the respondents' opinions towards the items of the seventh field "***System Access Control***". The following facts could be concluded:

- The statistical mean for item (4) equals (8.57), the weight mean equals (85.70%) and the sig. (p-value) equals (0.000), less than ($\alpha = 0.05$), which shows statistical significance and that the response level of this item is strongly greater than the neutrality degree of (6). This implies that the respondents strongly agree that "*A unique identifier is provided to every user (There are not public accounts used by more than one user)*". The finding agrees with Saleh & Alfantookh (2011) in their study about a new comprehensive framework for enterprise information security risk management as said there is an important need of using a management criteria and permits various criterion to be taken into account. This result also agrees with what Tayeh (2008) has found in his study about the effectiveness of information security management at the Palestinian IT companies, where the response weight mean equaled (%79.27) over this item. This fact could be attributed to the IT staff awareness reflected in dedicating a unique identifier for every individual in order to define the personal responsibilities.
- The statistical mean for item (3) equals (6.69), the weight mean equals (66.90%) and the sig. (p-value) equals (0.000), less than ($\alpha = 0.05$), which shows statistical significance and that the response level of this item is greater than the neutrality degree of (6). This implies that the respondents agree that "*There are some guidelines in place to guide users in selecting and maintaining secure passwords*". The finding agrees with Seleznyov & Puuronen (2003) in their study using continuous user authentication to detect masqueraders as they found that there are temporal patterns in user behavior and they may be used as well as sequential ones to efficiently detect anomalies in user behavior. The finding also agrees with Irakleous (2002) in the study about an experimental comparison of secret-based user authentication technologies as concluded that while passwords and PIN approaches good ratings on basis of their existing familiarity to participants, other methods based upon image recall and cognitive questions also achieved sufficiently positive results to suggest them as viable alternatives in certain context. This result also agrees with what Tayeh (2008) has found in his study

about the effectiveness of information security management in the Palestinian IT companies, where the response weight mean equaled (%69.51) over this item.

- In general, the statistical mean for the whole field "*System Access Control*" equals (7.47), the weight mean equals (74.70%) and the sig. (p-value) equals (0.000) less than ($\alpha = 0.05$), which shows that the response level of this field is greater than the neutrality degree of (6). This reveals that the respondents agree with the field "*System Access Control*". This result agrees with the study of Tayeh (2008) where he has found the response weight of the effect of the system access control on the effectiveness of information security management at the Palestinian IT companies equals (73.11%). This fact requires the government to exert more efforts in enhancing the system access control management by proceeding effective procedures to review and evaluate user access rights and privileges and establishing security policy that defines the rules and rights for each user. This also agrees with Hong and others (Hong K. , Chi, Chao, & Tang, 2003) that security is to combine systems, operations, and internal controls to ensure integrity and confidentiality of data and operation procedures in an organization. Authors also added that with the arrival of information technology, users' roles in information systems have evolved from IT specialists for access information facilities, to non-IT personnel for regular operations, to unspecified individuals from outside.

5.3.2.1.8 Field Eight: Systems Development and Maintenance

Table (5.16) shows the respondents' opinions towards the items of the eighth field "***Systems Development and Maintenance***". The following facts could be concluded:

- The statistical mean for item (1) equals (7.72), the weight mean equals (77.20%) and the sig. (p-value) equals (0.000), less than ($\alpha = 0.05$), which shows statistical significance and that the response level of this item is greater than the neutrality degree of (6). This implies that the respondents agree that "*The data input to application system is validated to ensure that it is correct and appropriate*". This result agrees with what Tayeh (2008) has found in his study about the effectiveness of information security management in the Palestinian IT companies, where the

response weight mean equaled (%79.27) over this item. This fact could be attributed to the IT staff awareness reflected in developing and maintaining application systems regarding the availability and integrity perspectives.

Table (5.16)
One-Sample T test mean and P-value (sig.) of
the eighth field: Systems Development and Maintenance

No.	Item (question)	Mean	Weight Mean	P-value (sig.)	Test Value (T)	Order
1	The data input to application system is validated to ensure that it is correct and appropriate.	7.72	77.20	0.000	12.162	1
2	The data output of application system is validated to ensure that the processing of stored information is correct and appropriate.	7.72	77.20	0.000	13.058	2
3	Encryption techniques were used to protect the data.	7.23	72.30	0.000	7.076	3
4	There are some controls in place for the execution of software on operating systems. This is to minimize the risk of corrupting operating systems.	7.11	71.10	0.000	6.748	4
5	There are strict control procedures in place over executing any changes to the information systems to minimize the corruption of them.	6.94	69.40	0.000	5.946	5
All the items of the field		7.34	73.40	0.000	10.622	

(Statistical Significance at level $\alpha = 0.05$)

- The statistical mean for item (5) equals (6.94), the weight mean equals (69.40%) and the sig. (p-value) equals (0.000), less than ($\alpha = 0.05$), which shows statistical significance and that the response level of this item is greater than the neutrality degree of (6). This indicates that the respondents agree that "*There are strict control procedures in place over executing any changes to the information systems to minimize the corruption of them*". This result agrees with what Tayeh (2008) has found in his study about the effectiveness of information security management in the Palestinian IT companies, where the response weight mean equaled (%75.00) over this item. This result shows the IT staff awareness reflected in developing and maintaining application systems regarding the availability and integrity perspectives.
- In general, the statistical mean for the whole field "*Systems Development and Maintenance*" equals (7.34), the weight mean equals (73.40%) and the sig. (p-

value) equals (0.000) less than (α = 0.05), which shows that the response level of this field is greater than the neutrality degree of (6). This reveals that the respondents agree with the field "*Systems Development and Maintenance*". This result agrees with the study Tayeh (2008) where he has found the response weight of the effect of the systems development and maintenance field on the effectiveness of information security management in the Palestinian IT companies equals (74.39%). This fact requires the government to exert more efforts in enhancing the systems development and maintenance by proceeding effective procedures to ensure the availability and integrity perspectives of the organization information systems. This also agrees with Grance, Hash, & Stevens (2004) whom stated that including security early in the information system development life cycle (SDLC) will usually result in less expensive and more effective security than adding it to an operational system.

5.3.2.1.9 Field Nine: Business Continuity Planning

Table (5.17)
One-Sample T test mean and P-value (sig.) of the ninth field: Business Continuity Planning

No.	Item (question)	Mean	Weight Mean	P-value (sig.)	Test Value (T)	Order
1	There is a managed process in place for developing and maintaining work continuity throughout the organization.	7.60	76.00	0.000	12.036	1
2	The events that could cause interruptions to work process were identified.	7.01	70.10	0.000	6.669	2
3	Plans were developed to restore business operations within the required time frame following an interruption or failure to work process.	6.85	68.50	0.000	4.994	3
4	Work continuity plans are tested regularly to ensure that they are up to date and effective.	6.51	65.10	0.003	2.975	4
All the items of the field		6.99	69.90	0.000	7.417	

(Statistical Significance at level α = 0.05)

Table (5.17) shows the respondents' opinions towards the items of the ninth field "***Business Continuity Planning***". The following facts could be concluded:

- The statistical mean for item (1) equals (7.60), the weight mean equals (76.00%) and the sig. (p-value) equals (0.000), less than (α = 0.05), which shows statistical significance and that the response level of this item is greater than the neutrality degree of (6). This implies that the respondents agree that "*There is a managed process in place for developing and maintaining work continuity throughout the organization*". This finding agrees with Ammar (2009) that found the response weight mean equaled (%75.66) for the item in his study *"top management keep pace with the technical developments".* This result also agrees with what Tayeh (2008) has found in his study about the effectiveness of information security management in the Palestinian IT companies, where the response weight mean equaled (%70.73) over this item. This fact could be attributed to the planning procedures managed by the organization to ensure work continuity, especially at conditions plenty with events that could cause interruptions to work process.
- The statistical mean for item (4) equals (6.51), the weight mean equals (65.10%) and the sig. (p-value) equals (0.003), less than (α = 0.05), which shows statistical significance and that the response level of this item is greater than the neutrality degree of (6). This implies that the respondents agree that "*Work continuity plans are tested regularly to ensure that they are up to date and effective*". This result agrees with what Tayeh (2008) has found in his study about the effectiveness of information security management in the Palestinian IT companies, where the response weight mean equaled (%62.20) over this item. It could be concluded from this result that the government is required to ensure testing the continuity plans regularly.
- In general, the statistical mean for the whole field "*Business Continuity Planning*" equals (6.99), the weight mean equals (69.90%) and the sig. (p-value) equals (0.000) less than (α = 0.05), which shows that the response level of this field is greater than the neutrality degree of (6). This implies that the respondents agree with the field "*Business Continuity Planning*". The finding agrees with the study of Kwon, Jang, Lee, & Ki (2007) that studied the common defects in information security management system of Korean companies, as they outlined the issues to be attended to among enterprises at each stage of the establishment of the ISMS

and presented a reference model for conducting a self-assessment, so that companies may be able to self-verify the completeness of their establishment of the ISMS. This result also agrees with the study of Tayeh (2008) where he has found the response weight of the effect of business continuity planning field on the effectiveness of information security management in the Palestinian IT companies equals (66.34%). This fact requires the government to exert more efforts in enhancing the business continuity planning by proceeding effective procedures to ensure the work continuity, avoid the potential events that cause interruptions in work process, restore work processes when interruptions take place and testing the work continuity plans regularly. This also agrees, to some extent with the study of Botha & Solms (2004) which stated that the small and medium organizations could prove difficult of developing a business continuity plan.

5.3.2.1.10 Field Ten: Compliance to Legal Requirements

Table (5.18)
One-Sample T test mean and P-value (sig.) of the tenth field: Compliance to Legal Requirements

No.	Item (question)	Mean	Weight Mean	P-value (sig.)	Test Value (T)	Order
1	All relevant statutory, regulatory and contractual requirements were explicitly defined and documented for each information system.	6.10	61.00	0.575	0.562	2
2	Specific controls and individual responsibilities to meet these requirements were defined and documented.	6.13	61.30	0.458	0.744	1
3	There exist and well implemented some procedures to ensure compliance with legal restrictions on use of material in respect of which there may be intellectual property rights (copyright, design rights, trade marks).	5.52	55.20	0.016	-2.443	3
4	All areas within the organization are considered for regular review to ensure compliance with security policy, standards and procedures.	5.44	54.40	0.004	-2.952	4
All the items of the field		5.80	58.00	0.241	-1.177	

(Statistical Significance at level $\alpha = 0.05$)

Table (5.18) shows the respondents' opinions towards the items of the tenth field "***Compliance to Legal Requirements***". The following facts could be concluded:

- The statistical mean for item (2) equals (6.13), the weight mean equals (61.30%) and the sig. (p-value) equals (0.458), greater than ($\alpha = 0.05$), which does not show statistical significance and reveals that the response level of this item approaches the neutrality degree of (6). This result agrees with what Tayeh (2008) has found in his study about the effectiveness of information security management in the Palestinian IT companies, where the response weight mean equaled (%62.20) over this item. This fact requires the government to enforce defining individual responsibilities and the related controls to meet the legal requirements.
- The statistical mean for item (4) equals (5.44), the weight mean equals (54.40%) and the sig. (p-value) equals (0.004), less than ($\alpha = 0.05$), which shows statistical significance and that the response level of this item is less than the neutrality degree of (6). This indicates that the respondents do not agree that "*All areas within the organization are considered for regular review to ensure compliance with security policy, standards and procedures*". The finding agrees with Luthy & Forcht (2006) in their study about laws and regulations affecting information management and frameworks for assessing compliance, as they found that organizations worldwide are impacted by an increasing number of laws and regulations. This result does not agree with what Tayeh (2008) has found in his study about the effectiveness of information security management in the Palestinian IT companies, where the response weight mean equaled (%63.41) over this item. It could be concluded from this result that the government should consider all areas within the institution to ensure compliance with security policy and standards.
- In general, the statistical mean for the whole field "*Compliance to Legal Requirements*" equals (5.80), the weight mean equals (58.00%) and the sig. (p-value) equals (0.241) greater than ($\alpha = 0.05$), which shows that the response level of this field is less than the neutrality degree of (6). This implies that the respondents disagree with the field "*Compliance to Legal Requirements*". The finding agrees with Ozkan & Karabacak (2010) in their study about a collaborative risk method for information security management practices: A case context within Turkey as they found a fundamental issue is that there is no legislation that regulates the information security liabilities of the public

organizations in Turkey .This result disagrees with the study of Tayeh (2008), where he has found the response weight of the effect of the compliance to legal requirements field on the effectiveness of information security management in the Palestinian IT companies equals (67.25%). This fact requires the government to consider all areas within the institution to ensure compliance with security policy and standards and to enforce defining individual responsibilities and the related controls to meet the legal requirements. This result also agrees, to some extent with the study of Luthy & Forcht (2006) which stated that organizations worldwide lack explicit references to information management. The authors also added that awareness of applicable laws and regulations, along with their potential impacts on information management systems, is critical for compliance.

5.3.2.1.11: Overall Fields of Information Security Management

Table (5.19)
One-Sample T test mean and P-value (sig.) of the overall fields of Information Security Management

No.	Field	Mean	Weight Mean	P-value (sig.)	Test Value (T)	Order
1	Security Policy	6.63	66.30	0.000	4.167	6
2	Organizational Security	5.60	56.00	0.004	-2.891	9
3	Asset Classification and Control	6.00	60.00	1.000	.000	7
4	Personnel Security	5.34	53.40	0.000	-3.956	10
5	Physical and Environmental Security	7.31	73.10	0.000	9.907	3
6	Computer and Network Management	6.93	69.30	0.000	7.941	5
7	System Access Control	7.47	74.70	0.000	12.730	1
8	Systems Development and Maintenance	7.34	73.40	0.000	10.622	2
9	Business Continuity Planning	6.99	69.90	0.000	7.417	4
10	Compliance to Legal Requirements	5.80	58.00	0.241	-1.177	8
All Information Security Management Fields		6.53	65.30	0.000	4.884	

(Statistical Significance at level $\alpha = 0.05$)

Table (5.19) shows the respondents' opinions towards the overall fields of information security management as they are ranked in a descending order according to the acceptance degree, where the rank (1) represents the field that has the highest acceptance degree. In general, the statistical mean for the whole fields equals (6.53), the weight mean equals (65.30%) and the sig. (p-value) equals (0.000) less than ($\alpha = 0.05$), which shows that the overall response level with regard to these fields is greater than the neutrality degree of (6). This indicates that the respondents agree with information security management fields generally. On the other hand, there are clear weaknesses in some fields like: "*Personnel Security*", "*Organizational Security*", "*Compliance to Legal Requirements*" and "*Asset Classification and Control*". This fact requires the government to consider all areas within these fields and try to improve the potential drawbacks.

5.3.2.2 Analysis of Electronic Management Field (Effectiveness of Applying e-Management)

Table (5.20) shows the respondents' opinions towards the items of the third part "***Effectiveness of Applying e-Management***". The following facts could be concluded:

- The statistical mean for item (14) equals (8.59), the weight mean equals (85.90%) and the sig. (p-value) equals (0.000), less than ($\alpha = 0.05$), which shows statistical significance and that the response level of this item is strongly greater than the neutrality degree of (6). This implies that the respondents strongly agree that "*The information back-up copies are kept in safe places out the organization*". This result agrees with what Al-Aloul (2011) has found in his study about keeping information back-up copies in safe places out the institution, where the response weight mean equaled (%70.30) over this item. This fact reflects the institution's IT staff awareness about the value of information and considering it as a valuable asset deserves the perfect preservation.

Table (5.20)
One-Sample T test mean and P-value (sig.) of
the third part: Effectiveness of Applying e-Management

No.	Item (question)	Mean	Weight Mean	P-value (sig.)	Test Value (T)	Order
1	Top management supports applying e-management in the organization.	8.22	82.20	0.000	14.269	2
2	There is a special and appropriate team in place to apply e-management at the organization.	7.99	79.90	0.000	13.041	5
3	The personnel accept the implementation of the e-management at the organization.	7.48	74.80	0.000	10.074	8
4	The personnel have the appropriate knowledge and experience to deal with applying the e-management.	7.00	70.00	0.000	6.417	10
5	The personnel take the needed training on technical tools according to their job needs.	6.92	69.20	0.000	6.087	11
6	The internal administration procedures are done simply without any sophistication.	6.76	67.60	0.000	4.478	13
7	The procedures to serve the out of organization stakeholders are done simply and without any sophistication.	6.76	67.60	0.000	5.046	14
8	There are self-resources in place to ensure the continuity and development of applying the e-management at the strategic term.	6.56	65.60	0.001	3.382	15
9	The organization stakeholders accept to deal with the organization via its internet website.	6.82	68.20	0.000	5.316	12
10	There exist at the organization a lot of the technical requirements like (computers, network, server, hard disks, internet, software and systems).	8.21	82.10	0.000	15.693	3
11	The software applications deliver the sufficient and accurate information properly.	7.67	76.70	0.000	12.629	6
12	The e-management creates a secure environment to exchange information.	7.63	76.30	0.000	12.216	7
13	There exists an effective system to define the authorized users to access the computerized information.	8.08	80.80	0.000	16.448	4

No.	Item (question)	Mean	Weight Mean	P-value (sig.)	Test Value (T)	Order
14	The information back-up copies are kept in safe places out the organization.	8.59	85.90	0.000	20.817	1
15	There exist clear and black policies for the personnel who violate the information confidentiality and security.	7.05	70.50	0.000	6.069	9
All the items of the field		7.45	74.50	0.000	15.453	

(Statistical Significance at level $\alpha = 0.05$)

- The statistical mean for item (1) equals (8.22), the weight mean equals (82.20%) and the sig. (p-value) equals (0.000), less than ($\alpha = 0.05$), which shows statistical significance and that the response level of this item is greater than the neutrality degree of (6). This indicates that the respondents agree that "*The top management supports applying e-management in the organization*". This finding agrees with the study of Al-Ajez (2011) that studied the role of the organizational culture on applying e-management effectively in the Palestinian ministry of higher education as it found that the top management supports applying e-management in the administrative environment, where the response weight mean equaled (67.84%). This result also agrees with what Al-Aloul (2011) has found in his study about the top management support to apply the e-management at the organization, where the response weight mean equaled (%81.80) over this item. This fact could be attributed to the high awareness among the top management about the valuable features of applying the e-management.
- The statistical mean for item (8) equals (6.56), the weight mean equals (65.60%) and the sig. (p-value) equals (0.001), less than ($\alpha = 0.05$), which shows statistical significance and that the response level of this item is moderately greater than the neutrality degree of (6). This implies that the respondents moderately agree that "*There are self-resources in place to ensure the continuity and development of applying e-management at the strategic term*". This finding agrees with Al-Ajez (2011) that said the top management supports the sustainable development process in applying e-management in the Palestinian ministry of high education. This result

disagrees with what Al-Aloul (2011) has found in his study about the organization ability to ensure the continuity and development of applying the e-management at the strategic term, where the response weight mean equaled (%50.20) over this item.

- The statistical mean for item (7) equals (6.76), the weight mean equals (67.60%) and the sig. (p-value) equals (0.000), less than ($\alpha = 0.05$), which shows statistical significance and that the response level of this item is greater than the neutrality degree of (6). This implies that the respondents agree that "*The procedures to serve the out of organization stakeholders are done simply and without any sophistication*". This result agrees with what Al-Aloul (2011) has found in his study about serving the stakeholders with simple procedures in the organization, where the response weight mean equaled (%83.40) over this item. This finding also agrees with Al-Ajez (2011) that said there was a utilization of information feedback allowed by the ministry website about the stakeholders preferences as the response mean weight was (%69.96). This fact could be attributed to the availability of simple administrative measures modified to fit the electronic environment without sophistication.
- In general, the statistical mean for the whole part "*Effectiveness of Applying e-Management*" equals (7.45), the weight mean equals (74.50%) and the sig. (p-value) equals (0.000) less than ($\alpha = 0.05$), which shows that the response level of this field is greater than the neutrality degree of (6). This implies that the respondents agree with the third part "*Effectiveness of Applying e-Management*". This finding disagrees with the study of Al-Somairy (2009) that found the response weight mean equaled (%50.27) in studying the requirements of applying e-management in the secondary schools in Gaza. This result is also better than what has been found at the study Al-Aloul(2011), where he has found the response weight due to the available requirements for successful implementation of e-management at charitable associations equals (68.92%).

5.3.3 Hypothesis Testing:

5.3.3.1 First Main Hypothesis Testing and testing its sub-hypothesis:

The Pearson Correlation Coefficient test was used to examine the correlation significance in testing the first main hypothesis via its subsidiary ones as the following:

Null Hypothesis: There is no significant statistical correlation at level ($\alpha = 0.05$) between the fields of information security management and the effectiveness of applying e-management in the Governmental Institutions in Gaza.

Alternative Hypothesis: There is a significant statistical correlation at level ($\alpha = 0.05$) between the fields of information security management and the effectiveness of applying e-management in the Governmental Institutions in Gaza.

If the sig. (p-value) was greater than the significance level at ($\alpha = 0.05$), then we could not reject the null hypothesis and this reveals that there does not exist a significant statistical correlation between the fields of information security management and the effectiveness of applying e-management in the Governmental Institutions in Gaza. If the sig. (p-value) was less than or equaled the significance level at ($\alpha = 0.05$), then we should reject the null hypothesis and accept the alternative one. This confirms that there exists a significant statistical correlation between the fields of information security management and the effectiveness of applying e-management in the Governmental Institutions in Gaza. Indeed, the Pearson Correlation Coefficient test was applied for each field of information security management separately.

5.3.3.1.1 Sub-Hypothesis One Testing:

Hypothesis One: *There is a significant statistical correlation at level ($\alpha = 0.05$) between the Security Policy and the effectiveness of applying e-management in the Governmental Institutions in Gaza.*

This hypothesis was tested by applying the Pearson Correlation Coefficient test on the items of the first field "***Security Policy***" and the items of the third part "***Effectiveness of Applying e-Management***".

Table (5.21)
The correlation coefficient between
"*Security Policy*" and "*Effectiveness of Applying e-Management*"

Field	Pearson correlation coefficient	P-value (sig.)
Security Policy	0.413**	0.000

** (Indicates Correlation Significance at α = 0.01)

Table (5.21) shows that the correlation coefficient between "***Security Policy***" and "***Effectiveness of Applying e-Management***" equals (0.413), and the p-value (sig.) equals (0.000) which is less than (α = 0.05). This result confirms a positive relation indicating a statistical significance between "***Security Policy***" and "***Effectiveness of Applying e-Management***". This result agrees with the study of Tayeh(2008) that said there is a significant effect for written information security policy on the effectiveness of information security management in the Palestinian information technology companies.

It could be concluded from the last result that this positive relation is referred to the following points:

- There is a known and defined responsible department for information security policy and its review, maintenance and upgrade.
- The maintenance and review process considers any new affecting changes like: significant security incidents, news risks, changes in organizational or technical infrastructure.
- The existed information security policy states how the organization follows an effective approach to manage information security.

5.3.3.1.2 Sub-Hypothesis Two Testing:

Hypothesis Two: *There is a significant statistical correlation at level (α = 0.05) between the Organizational Security and the effectiveness of applying e-management in the Governmental Institutions in Gaza.*

This hypothesis was tested by applying the Pearson Correlation Coefficient test on the items of the second field "***Organizational Security***" and the items of the third part "***Effectiveness of Applying e-Management***".

Table (5.22)
The correlation coefficient between
"*Organizational Security*" and "*Effectiveness of Applying e-Management*"

Field	Pearson correlation coefficient	P-value (sig.)
Organizational Security	0.343**	0.000

** (Indicates Correlation Significance at α = 0.01)

Table (5.22) shows that the correlation coefficient between "***Organizational Security***" and "***Effectiveness of Applying e-Management***" equals (0.343), and the p-value (sig.) equals (0.000) which is less than (α = 0.05). This result confirms a positive relation indicating a statistical significance between "***Organizational Security***" and "***Effectiveness of Applying e-Management***". This finding agrees with Al-Otaibi (2010) that found a compatibility degree of the (Information security' strategies) and (Organizing the information security) in websites of both sectors: civil and security ones with the local and international standards. This result also agrees with the study of Tayeh (2008) that said there is a significant effect for organizational security structure on the effectiveness of information security management in Palestinian information technology companies. This result also agrees with the study of Al-Ajez (2011) that stated there is a significant positive relation between the organizational values and the effective implementation of e-management in the Palestinian ministry of high education.

It could be concluded from the last result that this positive relation is referred to the following points:

- Responsibilities for the protection of individual informatics assets and for carrying out specific security processes were clearly defined.
- There is a cross-functional forum of management representatives from relevant parts of the institution to coordinate the implementation of information security controls.

- Specialized information security advice is obtained where appropriate.

5.3.3.1.3 Sub-Hypothesis Three Testing:

Hypothesis Three: *There is a significant statistical correlation at level (α = 0.05) between the Asset Classification and Control and the effectiveness of applying e-management in the Governmental Institutions in Gaza.*

This hypothesis was tested by applying the Pearson Correlation Coefficient test on the items of the third field "***Asset Classification and Control***" and the items of the third part "***Effectiveness of Applying e-Management***".

Table (5.23)
The correlation coefficient between
"*Asset Classification and Control*" and "*Effectiveness of Applying e-Management*"

Field	Pearson correlation coefficient	P-value (sig.)
Asset Classification and Control	0.402**	0.000

** (Indicates Correlation Significance at α = 0.01)

Table (5.23) shows that the correlation coefficient between "***Asset Classification and Control***" and "***Effectiveness of Applying e-Management***" equals (0.402), and the p-value (sig.) equals (0.000) which is less than (α = 0.05). This result confirms a positive relation indicating a statistical significance between "***Asset Classification and Control***" and "***Effectiveness of Applying e-Management***". This finding agrees with Al-Somairy (2009) that found there was a correlation between the material requirements availability level and the effective implementation of e-management. This result also agrees with the study Tayeh (2008) that said there is a significant effect for asset classification and control on the effectiveness of information security management in the Palestinian information technology companies.

It could be concluded from the last result that this positive relation is referred to the following points:

- The institution uses a data record file to identify the important assets associated with each information system.

- An appropriate set of procedures are defined for information labeling and handling in accordance with the classification scheme adopted by the institution.
- There is an Information classification scheme or guideline in place; which will assist in determining how the information is to be handled and protected.

5.3.3.1.4 Sub-Hypothesis Four Testing:

Hypothesis Four: *There is a significant statistical correlation at level (α = 0.05) between the Personnel Security and the effectiveness of applying e-management in the Governmental Institutions in Gaza.*

This hypothesis was tested by applying the Pearson Correlation Coefficient test on the items of the fourth field "***Personnel Security***" and the items of the third part "***Effectiveness of Applying e-Management***".

Table (5.24)
The correlation coefficient between
"*Personnel Security*" and "*Effectiveness of Applying e-Management*"

Field	Pearson correlation coefficient	P-value (sig.)
Personnel Security	0.375**	0.000

** (Indicates Correlation Significance at α = 0.01)

Table (5.24) shows that the correlation coefficient between "***Personnel Security***" and "***Effectiveness of Applying e-Management***" equals (0.375), and the p-value (sig.) equals (0.000) which is less than (α = 0.05). This result confirms a positive relation indicating a statistical significance between "***Personnel Security***" and "***Effectiveness of Applying e-Management***". This finding agrees with Ammar (2009) that said the effective implementation of e-management contributes to increase the security awareness among personnel. This result also agrees with the study of Tayeh (2008) that said there is a significant effect for applying personnel security on the effectiveness of information security management in Palestinian information technology companies. This result also agrees with the study of Al-Ajez (2011) that there is a significant positive relation between the organizational values and beliefs and the effective implementation of e-management in the Palestinian ministry of high education.

It could be concluded from the last result that this positive relation is referred to the following points:

- Employees are asked to sign confidentiality or nondisclosure agreement as a part of their initial terms and conditions of the employment.
- There is a formal disciplinary process in place for employees who have violated organizational security policies and procedures.
- Security roles and responsibilities as laid in the organization security policy are documented in the employee job description card.

5.3.3.1.5 Sub-Hypothesis Five Testing:

Hypothesis Five: *There is a significant statistical correlation at level (α = 0.05) between the Physical and Environmental Security and the effectiveness of applying e-management in the Governmental Institutions in Gaza.*

This hypothesis was tested by applying the Pearson Correlation Coefficient test on the items of the fifth field "***Physical and Environmental Security***" and the items of the third part "***Effectiveness of Applying e-Management***".

Table (5.25)
The correlation coefficient between
"*Physical and Environmental Security*" and "*Effectiveness of Applying e-Management*"

Field	Pearson correlation coefficient	P-value (sig.)
Physical and Environmental Security	0.519**	0.000

** (Indicates Correlation Significance at α = 0.01)

Table (5.25) shows that the correlation coefficient between "***Physical and Environmental Security***" and "***Effectiveness of Applying e-Management***" equals (0.519), and the p-value (sig.) equals (0.000) which is less than (α = 0.05). This result confirms a positive relation indicating a statistical significance between "***Physical and Environmental Security***" and "***Effectiveness of Applying e-Management***". This finding

agrees with Ammar (2009) that said there is a correlation between the environmental security dimensions and the effective implementation of e-management. This result also agrees with the study of Tayeh (2008) that said there is a significant effect for applying physical and environmental security on the effectiveness of information security management in the Palestinian information technology companies.

It could be concluded from the last result that this positive relation is referred to the following points:

- The equipment is protected from power failures by using permanence power supplies such as multiple feeds, UPS, backup generator etc.
- The rooms, which have the information processing service, are locked or have lockable cabinets or safes.

5.3.3.1.6 Sub-Hypothesis Six Testing:

Hypothesis Six: *There is a significant statistical correlation at level (α = 0.05) between Computer and Network Management and the effectiveness of applying e-management in the Governmental Institutions in Gaza.*

This hypothesis was tested by applying the Pearson Correlation Coefficient test on the items of the sixth field "***Computer and Network Management***" and the items of the third part "***Effectiveness of Applying e-Management***".

Table (5.26)
The correlation coefficient between
"*Computer and Network Management*" and "*Effectiveness of Applying e-Management*"

Field	Pearson correlation coefficient	P-value (sig.)
Computer and Network Management	0.639**	0.000

** (Indicates Correlation Significance at α = 0.01)

Table (5.26) shows that the correlation coefficient between "***Computer and Network Management***" and "***Effectiveness of Applying e-Management***" equals (0.639), and the p-value (sig.) equals (0.000) which is less than (α = 0.05). This result confirms a positive relation indicating a statistical significance between "***Computer and Network***

Management" and "***Effectiveness of Applying e-Management***". This finding agrees with Al-Aloul (2011) that said there is a correlation between the material and equipment requirements and the effective implementation of e-management. This result also agrees with the study of Tayeh (2008) that said there is a significant effect for computer and network management on the effectiveness of information security management in the Palestinian information technology companies.

It could be concluded from the last result that this positive relation is referred to the following points:

- The security policy has identified any operating procedures such as back-up, equipment maintenance etc.
- Antivirus software is installed on the computers to check and remove any viruses from computers and media and this software signature is updated regularly.
- System acceptance criteria are established for new information systems, upgrades and new versions and suitable tests were carried out prior to acceptance.
- Duties and responsibilities about systems and equipment are separated in order to reduce opportunities for unauthorized modification or misuse of information or services.
- Audit logs are maintained for any change made to the operating programs.

5.3.3.1.7 Sub-Hypothesis Seven Testing:

Hypothesis Seven: *There is a significant statistical correlation at level ($\alpha = 0.05$) between System Access Control and the effectiveness of applying e-management in the Governmental Institutions in Gaza.*

This hypothesis was tested by applying the Pearson Correlation Coefficient test on the items of the seventh field "***System Access Control***" and the items of the third part "***Effectiveness of Applying e-Management***".

Table (5.27)
The correlation coefficient between
"*System Access Control*" and "*Effectiveness of Applying e-Management*"

Field	Pearson correlation coefficient	P-value (sig.)
System Access Control	0.612**	0.000

** (Indicates Correlation Significance at α = 0.01)

Table (5.27) shows that the correlation coefficient between "***System Access Control***" and "***Effectiveness of Applying e-Management***" equals (0.612), and the p-value (sig.) equals (0.000) which is less than (α = 0.05). This result confirms a positive relation indicating a statistical significance between "***System Access Control***" and "***Effectiveness of Applying e-Management***". This result agrees with the study of Tayeh (2008) that said there is a significant effect for system access control on the effectiveness of information security management in the Palestinian information technology companies. In addition, this finding agrees with Ammar (2009) that found a correlation between user authentication and the effective implementation of e-management.

It could be concluded from the last result that this positive relation is referred to the following points:

- A unique identifier is provided to every user (There are not public accounts used by more than one user).
- The access control policy does address the rules and rights for each user or a group of users.
- The sensitive systems are provided with isolated computing environment such as running on a dedicated computer, share resources only with trusted application systems.
- An audit logs recording security relevant events are produced and kept for an agreed period to assist in future investigations and access control monitoring.

5.3.3.1.8 Sub-Hypothesis Eight Testing:

Hypothesis Eight: *There is a significant statistical correlation at level (α = 0.05) between Systems Development and Maintenance and the effectiveness of applying e-management in the Governmental Institutions in Gaza.*

This hypothesis was tested by applying the Pearson Correlation Coefficient test on the items of the eighth field "***Systems Development and Maintenance***" and the items of the third part "***Effectiveness of Applying e-Management***".

Table (5.28)
The correlation coefficient between
"*Systems Development and Maintenance*" and "*Effectiveness of Applying e-Management*"

Field	Pearson correlation coefficient	P-value (sig.)
Systems Development and Maintenance	0.509**	0.000

** (Indicates Correlation Significance at α = 0.01)

Table (5.28) shows that the correlation coefficient between "***Systems Development and Maintenance***" and "***Effectiveness of Applying e-Management***" equals (0.509), and the p-value (sig.) equals (0.000) which is less than (α = 0.05). This result confirms a positive relation indicating a statistical significance between "***Systems Development and Maintenance***" and "***Effectiveness of Applying e-Management***". This finding agrees with Al-Ghoty (2006) that said there is a correlation between the systems development and effective e-Government in Palestine. This result also agrees with the study of Tayeh (2008) that said there is a significant effect for systems development and maintenance on the effectiveness of information security management in the Palestinian information technology companies.

It could be concluded from the last result that this positive relation is referred to the following points:

- The data input to an application system is validated to ensure that it is correct and appropriate.

- The data output of an application system is validated to ensure that the processing of stored information is correct and appropriate.
- Encryption techniques were used to protect the data.
- There are some controls in place for the execution of software on operating systems. This is to minimize the risk of corrupting operating systems.

5.3.3.1.9 Sub-Hypothesis Nine Testing:

Hypothesis Nine: *There is a significant statistical correlation at level (α = 0.05) between the Business Continuity Planning and the effectiveness of applying e-management in the Governmental Institutions in Gaza.*

This hypothesis was tested by applying the Pearson Correlation Coefficient test on the items of the ninth field "***Business Continuity Planning***" and the items of the third part "***Effectiveness of Applying e-Management***".

Table (5.29)
The correlation coefficient between
"*Business Continuity Planning*" and "*Effectiveness of Applying e-Management*"

Field	Pearson correlation coefficient	P-value (sig.)
Business Continuity Planning	0.482**	0.000

** (Indicates Correlation Significance at α = 0.01)

Table (5.29) shows that the correlation coefficient between "***Business Continuity Planning***" and "***Effectiveness of Applying e-Management***" equals (0.482), and the p-value (sig.) equals (0.000) which is less than (α = 0.05). This result confirms a positive relation indicating a statistical significance between "***Business Continuity Planning***" and "***Effectiveness of Applying e-Management***". This result agrees with the study of Tayeh (2008) that said there is a significant effect for business continuity planning on the effectiveness of information security management in the Palestinian information technology companies. This result also agrees with the study of Al-Ajez (2011) that there is a significant positive relation between the organizational norms and expectations and

the effective implementation of e-management at the Palestinian ministry of high education.

It could be concluded from the last result that this positive relation is referred to the following points:

- There is a managed process in place for developing and maintaining work continuity throughout the institution.
- The events that could cause interruptions to work process were identified.
- Plans were developed to restore business operations within the required time frame following an interruption or failure to work process.

5.3.3.1.10 Sub-Hypothesis Ten Testing:

Hypothesis Ten: *There is a significant statistical correlation at level (α = 0.05) between Compliance to Legal Requirements and the effectiveness of applying e-management in the Governmental Institutions in Gaza.*

This hypothesis was tested by applying the Pearson Correlation Coefficient test on the items of the tenth field "***Compliance to Legal Requirements***" and the items of the third part "***Effectiveness of Applying e-Management***".

Table (5.30)
The correlation coefficient between
"*Compliance to Legal Requirements*" and "*Effectiveness of Applying e-Management*"

Field	Pearson correlation coefficient	P-value (sig.)
Compliance to Legal Requirements	0.398**	0.000

** (Indicates Correlation Significance at α = 0.01)

Table (5.30) shows that the correlation coefficient between "***Compliance to Legal Requirements***" and "***Effectiveness of Applying e-Management***" equals (0.398), and the p-value (sig.) equals (0.000) which is less than (α = 0.05). This result confirms a positive relation indicating a statistical significance between "***Compliance to Legal Requirements***" and "***Effectiveness of Applying e-Management***". This finding agrees with Luthy & Forcht (2006) in their study about laws and regulations affecting

information management and frameworks for assessing compliance, as they found that organizations worldwide are impacted by an increasing number of laws and regulations. This result also agrees with the study of Tayeh (2008) that said there is a significant effect for compliance to legal requirements on the effectiveness of information security management in the Palestinian information technology companies.

5.3.3.1.11 Main Hypothesis One Testing:

Main Hypothesis One: *There is a significant statistical correlation at level (α = 0.05) between the fields of information security management and the effectiveness of applying e-management in the Governmental Institutions in Gaza.*

This hypothesis was tested by applying the Pearson Correlation Coefficient test on the fields of "***Information Security Management***" and the third part "***Effectiveness of Applying e-Management***".

Table (5.31)
The correlation coefficient between
"*Information Security Management*" and "*Effectiveness of Applying e-Management*"

Field	Pearson correlation coefficient	P-value (sig.)
Information Security Management	0.612**	0.000

** (Indicates Correlation Significance at α = 0.01)

Table (5.31) shows that the correlation coefficient between "***Information Security Management***" and "***Effectiveness of Applying e-Management***" equals (0.612), and the p-value (sig.) equals (0.000) which is less than (α = 0.05). This result confirms a positive relation indicating a statistical significance between "***Information Security Management***" and "***Effectiveness of Applying e-Management***".

5.3.3.2 Second Main Hypothesis Testing and testing its sub-hypothesis:

In order to examine the second main hypothesis, the below described methodology was followed by setting a null hypothesis and an alternative one in an attempt to decide whether the null hypothesis could be rejected or not.

Null Hypothesis: There are no significant statistical differences at level (α = 0.05) among the respondents in their opinions about the impact of information security management on the effectiveness of applying e-management in the Governmental Institutions in Gaza attributed to their characteristic factors like (gender, qualification, specialty, age, job title, experience and the governmental institution they belong to).

Alternative Hypothesis: There are significant statistical differences at level (α = 0.05) among the respondents in their opinions about the impact of information security management on the effectiveness of applying e-management in the Governmental Institutions in Gaza attributed to their characteristic factors like (gender, qualification, specialty, age, job title, experience and the governmental institution they belong to).

If the sig. (p-value) was greater than the significance level at (α = 0.05), then we could not reject the null hypothesis and this implies that there are no significant statistical differences at level (α = 0.05) among the respondents in their opinions about the impact of information security management on the effectiveness of applying e-management in the Governmental Institutions in Gaza attributed to their characteristic factors. If the sig. (p-value) was less than or equaled the significance level at (α = 0.05), then we should reject the null hypothesis and accept the alternative one. This confirms that there are significant statistical differences at level (α = 0.05) among the respondents in their opinions about the impact of information security management on the effectiveness of applying e-management in the Governmental Institutions in Gaza attributed to their characteristic factors. Indeed, the appropriate statistical test was used according to the nature of the sample characteristic. For example: Two-independent samples T Test was used to determine if there are significant statistical differences between the means of two groups of data like the respondents' gender (male and female). On the other side, One-Way ANOVA test was used in the case of three groups of data and more like the respondents' level of qualification (general secondary, diploma, bachelor, master and Ph.D.).

To test this hypothesis, the following sub-hypotheses were examined.

5.3.3.2.1 Sub-Hypothesis One Testing:

Sub-Hypothesis One: *There are no significant statistical differences at level (α = 0.05) among the respondents in their opinions about the study fields attributed to their gender.*

This hypothesis was tested by applying Two-independent samples T Test on the study fields to determine if there are significant statistical differences at level (α = 0.05) among the respondents in their opinions over the study fields attributed to gender.

Table (5.32)
Two-independent samples T Test for testing the differences due to gender

No.	Field	Test Value (T)	P-value (sig.)	Mean	
				Male	Female
1	Security Policy	0.854	0.394	6.69	6.38
2	Organizational Security	-1.615	0.109	5.36	6.04
3	Asset Classification and Control	-0.097	0.923	5.99	6.03
4	Personnel Security	-0.945	0.346	5.26	5.65
5	Physical and Environmental Security	-0.291	0.772	7.29	7.39
6	Computer and Network Management	-0.452	0.652	6.90	7.03
7	System Access Control	-0.538	0.591	7.44	7.59
8	Systems Development and Maintenance	-0.710	0.479	7.30	7.52
9	Business Continuity Planning	-2.846	0.006	6.83	7.60
10	Compliance to Legal Requirements	-2.370	0.021	5.63	6.45
11	Information Security Management (All Fields)	-1.119	0.265	6.47	6.77
12	Effectiveness of Applying e-Management	-0.837	0.404	7.41	7.60

(Differences Denote Significance at Level α = 0.05)

Table (5.32) shows that the significance of all the study fields except the fields: "*Business Continuity Planning*" and "*Compliance to Legal Requirements*" is greater than the significance level (α = 0.05). This result indicates that there are no differences among the respondents in their opinions over the study fields attributed to gender. According to this result we can accept the sub-hypothesis "*There are no significant statistical differences at level (α = 0.05) among the respondents in their opinions about the study fields attributed to their gender*". Moreover, we can conclude that the study sample have a correspondent opinions over the study fields regardless of gender, and this confirms that gender does not

influence the study sample opinions towards the study fields. This result agrees with the study of Al-Ajez (2011) as he has found out that there were no differences among the respondents' opinions towards the role of the organizational culture on applying e-management effectively in the Palestinian ministry of higher education attributed to gender. It also agrees with the study of Zoarob(2009), which has studied the automation role in improving the performance of personnel affairs administration at the governmental ministries in Gaza. In addition, it agrees with the study of Al-Somairy (2009), which has studied the requirements of applying e-management at the secondary schools in Gaza and the developing methods. It also agrees with the study of Al-Aloul (2011), which has studied the available requirements for a successful implementation of e-management at the charitable associations in Gaza.

5.3.3.2.2 Sub-Hypothesis Two Testing:

Sub-Hypothesis Two: *There are no significant statistical differences at level (α = 0.05) among the respondents in their opinions about the study fields attributed to their qualification.*

This hypothesis was tested by applying One-Way ANOVA Test on the study fields to determine if there are significant statistical differences at level (α = 0.05) among the respondents in their opinions over the study fields attributed to the qualification level.

Table (5.33) shows that the significance of all study fields is greater than the significance level at (α = 0.05) except for the fields "*Personnel Security*", "*System Access Control*", "*Business Continuity Planning*" and "*Effectiveness of Applying e-Management*". In general, this result indicates that there are no differences among the respondents in their opinions over the study fields attributed to the qualification level. According to this result we can accept the sub-hypothesis "*There are no significant statistical differences at level (α = 0.05) among the respondents in their opinions over the study fields attributed to their qualification*".

Table (5.33)
One-Way ANOVA Test for testing the differences due to the qualification level

No.	Field	Test Value (F)	P-value (sig.)	Mean			
				General Secondary	Diploma	Bachelor	Master
1	Security Policy	0.141	0.936	7.13	6.53	6.64	6.48
2	Organizational Security	1.235	0. 299	6.13	5.56	5.57	4.33
3	Asset Classification and Control	2.169	0.094	7.00	5.85	6.12	4.50
4	Personnel Security	2.871	0.039	5.68	4.52	5.56	4.09
5	Physical and Environmental Security	1.700	0.170	6.89	6.54	7.43	7.49
6	Computer and Network Management	1.866	0.138	7.39	6.20	7.02	6.91
7	System Access Control	3.075	0.030	7.42	6.80	7.64	6.70
8	Systems Development and Maintenance	2.287	0.081	7.70	6.53	7.49	6.98
9	Business Continuity Planning	3.755	0.012	6.81	6.41	7.20	5.70
10	Compliance to Legal Requirements	2.106	0.102	6.88	5.54	5.92	4.45
11	Information Security Management (All Fields)	2.479	0.064	6.90	6.05	6.66	5.76
12	Effectiveness of Applying e-Management	3.016	0.032	7.07	6.87	7.60	6.95

(Differences Denote Significance at Level $\alpha = 0.05$)

Moreover, we can conclude that the study sample have a correspondent opinions over the study fields regardless of the qualification level, and this confirms that the qualification does not influence the study sample opinions towards the study fields. This result agrees with the study of Tayeh (2008), which has studied the effectiveness of information security management in the Palestinian IT companies. It also agrees with the study of Al-Ajez (2011), where he has found out that there are no differences among the

respondents' opinions towards the role of organizational culture on applying e-management effectively in the Palestinian ministry of higher education attributed to the respondents' qualification. In addition, this result agrees with Al-Somairy (2009), which has studied the requirements of applying e-management in the secondary schools in Gaza and the developing methods. On the other side, the result disagrees with Al-Aloul (2011), which has studied the available requirements for successful implementation of e-management in the charitable associations in Gaza.

5.3.3.2.3 Sub-Hypothesis Three Testing:

Sub-Hypothesis Three: *There are no significant statistical differences at level (α = 0.05) among the respondents in their opinions about the study fields attributed to their specialization.*

This hypothesis was tested by applying One-Way ANOVA Test on the study fields to determine if there are significant statistical differences at level (α = 0.05) among the respondents in their opinions over the study fields attributed to specialization.

Table (5.34) shows that the significance of all the study fields is greater than the significance level at (α = 0.05) except for the fields "*Personnel Security*" and "*Compliance to Legal Requirements*". This result indicates that there are no differences among the respondents in their opinions over the study fields attributed to specialization. According to this result we can accept the sub-hypothesis "*There are no significant statistical differences at level (α = 0.05) among the respondents in their opinions over the study fields attributed to their specialization*". Moreover, we can conclude that the study sample individuals have a correspondent opinion over the study fields regardless of the specialization, and this confirms that the specialization does not influence the study sample opinions towards the study fields.

Table (5.34)
One-Way ANOVA Test for testing the differences due to the specialization

No.	Field	Test Value (F)	P-value (sig.)	Mean					
				Computer Engineering	Computer Science	Information Technology	Business Administration	Electricity and Communication Engineer	Others
1	Security Policy	0.453	0.810	6.69	6.94	6.63	6.17	6.06	6.63
2	Organizational Security	1.503	0.193	5.05	5.49	5.63	5.42	5.75	6.36
3	Asset Classification and Control	1.234	0.296	5.62	5.92	5.82	6.17	6.13	6.82
4	Personnel Security	2.560	0.030	5.22	4.53	4.97	5.74	4.68	6.33
5	Physical and Environmental Security	0.836	0.526	7.46	7.06	6.98	7.81	7.36	7.08
6	Computer and Network Management	0.909	0.477	7.05	6.51	6.66	7.32	6.69	6.99
7	System Access Control	1.361	0.243	7.71	7.05	7.73	7.62	7.04	7.10
8	Systems Development and Maintenance	0.800	0.552	7.40	7.05	7.39	7.61	6.15	7.44
9	Business Continuity Planning	0.657	0.657	6.89	6.63	7.01	7.08	7.00	7.42
10	Compliance to Legal Requirements	2.376	0.042	5.30	5.63	5.65	6.18	5.56	6.84
11	Information Security Management (All Fields)	0.773	0.571	6.44	6.28	6.45	6.71	6.24	6.90
12	Effectiveness of Applying e-Management	0.584	0.712	7.64	7.39	7.35	7.32	6.97	7.34

(Differences Denote Significance at Level $\alpha = 0.05$)

5.3.3.2.4 Sub-Hypothesis Four Testing:

Sub-Hypothesis Four: *There are no significant statistical differences at level ($\alpha = 0.05$) among the respondents in their opinions about the study fields attributed to their age.*

This hypothesis was tested by applying One-Way ANOVA Test on the study fields to determine if there are significant statistical differences at level ($\alpha = 0.05$) among the respondents in their opinions over the study fields attributed to age.

Table (5.35)
One-Way ANOVA Test for testing the differences due to the age variable

No.	Field	Test Value (F)	P-value (sig.)	Mean		
				Below 30	30 to below 40	40 and more
1	Security Policy	2.415	0.093	6.78	6.24	7.27
2	Organizational Security	2.344	0.100	5.76	5.01	5.92
3	Asset Classification and Control	1.212	0.301	6.20	5.64	6.27
4	Personnel Security	2.022	0.136	5.44	4.99	6.15
5	Physical and Environmental Security	1.485	0.230	7.43	7.04	7.74
6	Computer and Network Management	1.958	0.145	7.05	6.65	7.37
7	System Access Control	3.670	0.028	7.71	7.07	7.67
8	Systems Development and Maintenance	4.483	0.013	7.48	6.93	8.18
9	Business Continuity Planning	3.233	0.042	7.16	6.58	7.62
10	Compliance to Legal Requirements	3.945	0.022	6.05	5.23	6.63
11	Information Security Management (All Fields)	4.480	0.013	6.71	6.14	7.08
12	Effectiveness of Applying e-Management	5.446	0.005	7.59	7.10	8.07

(Differences Denote Significance at Level $\alpha = 0.05$)

Table (5.35) shows that the significance for the study fields: "*Information Security Management (All Fields)"* and "*Effectiveness of Applying e-Management*" is less than the significance level at ($\alpha = 0.05$). This result indicates that there are differences among the respondents in their opinions over the study fields attributed to the age variable. According to this result we should reject the sub-hypothesis "*There are no significant statistical differences at level ($\alpha = 0.05$) among the respondents in their opinions over the study fields attributed to their age*". Moreover, we can conclude that the study sample individuals have a different vision over the study fields with regard to their age, and this confirms that the age does influence the study sample opinions towards the study fields.

This result disagrees with the study of Tayeh (2008), where he has found out that there are no differences among the respondents' opinions attributed to the company age in IT field. On the other side, this result agrees with the study of Al-Aloul (2011), which has studied the available requirements for successful implementation of e-management in the charitable associations in Gaza, and agrees with the study of Al-Ghoty (2006) which has studied the requirements for successful implementation of e-Government in the Palestinian ministries. To a large extent, the result disagrees with the study of Al-Ajez (2011), where he has found out that there are no differences among the respondents' opinions attributed to their age.

5.3.3.2.5 Sub-Hypothesis Five Testing:

Sub-Hypothesis Five: *There are no significant statistical differences at level (α = 0.05) among the respondents in their opinions about the study fields attributed to their experience.*

This hypothesis was tested by applying One-Way ANOVA Test on the study fields to determine if there are significant statistical differences at level (α = 0.05) among the respondents in their opinions over the study fields attributed to experience.

Table (5.36) shows that the significance for the study fields: "*Security Policy*", "*Physical and Environmental Security*", "*Computer and Network Management*", "*System Access Control*", "*Systems Development and Maintenance*" and "E*ffectiveness of Applying e-Management*" is greater than the significance level at (α = 0.05). This result indicates that there are no differences among the respondents in their opinions over these study fields attributed to the experience variable. According to this result we can accept the sub-hypothesis "*There are no significant statistical differences at level (α = 0.05) among the respondents in their opinions over the study fields attributed to their experience*" for the previously mentioned study fields. This result agrees with study of Al-Ajez (2011), where he has found out that there are no differences among the respondents' opinions attributed to their experience. It also agrees with the result of the study of Tayeh (2008).

Table (5.36)
One-Way ANOVA Test for testing the differences due to experience

No.	Field	Test Value (F)	P-value (sig.)	Mean		
				Below 4	4 to below 8	8 and more
1	Security Policy	1.290	0.279	6.85	6.34	6.74
2	Organizational Security	4.481	0.013	6.09	5.06	5.07
3	Asset Classification and Control	3.090	0.049	6.49	5.74	5.42
4	Personnel Security	7.017	0.001	6.00	4.68	5.26
5	Physical and Environmental Security	0.769	0.465	7.45	7.11	7.42
6	Computer and Network Management	1.280	0.281	7.10	6.70	7.05
7	System Access Control	1.436	0.241	7.66	7.24	7.52
8	Systems Development and Maintenance	1.791	0.171	7.38	7.11	7.79
9	Business Continuity Planning	4.723	0.010	7.30	6.50	7.36
10	Compliance to Legal Requirements	5.325	0.006	6.39	5.20	5.76
11	Information Security Management (All Fields)	4.527	0.012	6.87	6.17	6.54
12	Effectiveness of Applying e-Management	1.601	0.205	7.60	7.25	7.54

(Differences Denote Significance at Level $\alpha = 0.05$)

On the opposite side, Table (5.36) shows that the significance for the study fields: "*Organizational Security*", "*Asset Classification and Control*", "*Personnel Security*", "*Business Continuity Planning*", "*Compliance to Legal Requirements*" and "*Information Security Management (All Fields)*" is less than the significance level at ($\alpha = 0.05$). This result indicates that there are differences among the respondents in their opinions about these study fields with regard to the experience variable. According to this result we should reject the sub-hypothesis "*There are no significant statistical differences at level ($\alpha = 0.05$) among the respondents in their opinions over the study fields attributed to their experience*" for the previously mentioned study fields. This result agrees with the study of Al-Somairy (2009), which has studied the requirements of applying e-management in the secondary schools in Gaza and the developing methods.

5.3.3.2.6 Sub-Hypothesis Six Testing:

Sub-Hypothesis Six: *There are no significant statistical differences at level (α = 0.05) among the respondents in their opinions about the study fields attributed to their main work field.*

This hypothesis was tested by applying One-Way ANOVA Test on the study fields to determine if there are significant statistical differences at level (α = 0.05) among the respondents in their opinions over the study fields attributed to main work field.

Table (5.37)
One-Way ANOVA Test for testing the differences due to the main work field variable

No.	Field	Test Value (F)	P-value (sig.)	Mean		
				Management, Planning and Strategies Development	IT Related Units	Archiving and Information Management
1	Security Policy	0.494	0.611	7.14	6.56	6.62
2	Organizational Security	5.697	0.004	6.14	4.99	6.13
3	Asset Classification and Control	5.255	0.006	6.32	5.51	6.67
4	Personnel Security	4.939	0.008	5.90	4.88	5.91
5	Physical and Environmental Security	0.286	0.752	7.52	7.22	7.40
6	Computer and Network Management	1.741	0.179	7.61	6.79	7.00
7	System Access Control	1.781	0.172	8.15	7.49	7.30
8	Systems Development and Maintenance	2.219	0.112	8.22	7.20	7.38
9	Business Continuity Planning	2.870	0.060	7.93	6.78	7.12
10	Compliance to Legal Requirements	5.734	0.004	6.11	5.31	6.48
11	Information Security Management (All Fields)	3.901	0.022	7.10	6.27	6.80
12	Effectiveness of Applying e-Management	0.406	0.667	7.70	7.47	7.37

(Differences Denote Significance at Level α = 0.05)

Table (5.37) shows that the significance for the study fields: "*Security Policy*", "*Physical and Environmental Security*", "*Computer and Network Management*", "*System Access*

Control", "*Systems Development and Maintenance*" and "E*ffectiveness of Applying e-Management*" is greater than the significance level at (α = 0.05). This result indicates that there are no differences among the respondents in their opinions over the study fields with regard to the main work field variable. According to this result we can accept the sub-hypothesis "*There are no significant statistical differences at level (α = 0.05) among the respondents in their opinions over the study fields attributed to their main work field*" for the previously mentioned study fields. This result agrees with the result of the study of Tayeh (2008).

On the opposite side, Table (5.37) shows that the significance for the study fields: "*Organizational Security*", "*Asset Classification and Control*", "*Personnel Security*", "*Business Continuity Planning*", "*Compliance to Legal Requirements*" and "*Information Security Management (All Fields)*" is less than the significance level at (α = 0.05). This result indicates that there are differences among the respondents in their opinions over these study fields with regard to the main work field variable. According to this result we should reject the sub-hypothesis "*There are no significant statistical differences at level (α = 0.05) among the respondents in their opinions over the study fields attributed to the main work field*" for the previously mentioned study fields. This result agrees with the study of Al-Ajez (2011), where he has found out that there are differences among the respondents' opinions attributed to main work field.

5.3.3.2.7 Sub-Hypothesis Seven Testing:

Sub-Hypothesis Seven: *There are no significant statistical differences at level (α = 0.05) among the respondents in their opinions about the study fields attributed to the Governmental Institution they belong to.*

This hypothesis was tested by applying One-Way ANOVA Test on the study fields to determine if there are significant statistical differences at level (α = 0.05) among the respondents in their opinions over the study fields attributed to the governmental institution they belong to.

Table (5.38)
One-Way ANOVA Test for testing
The differences due to the governmental institution they belong to variable

No.	Field	Test Value (F)	P-value (sig.)
1	Security Policy	3.659	0.001
2	Organizational Security	1.824	0.087
3	Asset Classification and Control	1.479	0.180
4	Personnel Security	3.311	0.003
5	Physical and Environmental Security	2.979	0.006
6	Computer and Network Management	1.414	0.205
7	System Access Control	1.029	0.414
8	Systems Development and Maintenance	1.548	0.156
9	Business Continuity Planning	1.023	0.418
10	Compliance to Legal Requirements	1.376	0.221
11	Information Security Management (All Fields)	2.297	0.030
12	Effectiveness of Applying e-Management	2.582	0.016

(Differences Denote Significance at Level $\alpha = 0.05$)

Table (5.38) shows that the significance of the main study parts: "*Information Security Management (All Fields)*", "*Effectiveness of Applying e-Management*" is less than the significance level at ($\alpha = 0.05$). This result indicates that there are differences among the respondents in their opinions over the study fields with regard to the governmental institution they belong to. According to this result we should reject the sub-hypothesis "*There are no significant statistical differences at level ($\alpha = 0.05$) among the respondents in their opinions over the study fields attributed to the governmental institution they belong to*". Moreover, we can conclude that the study sample individuals have different opinions over the study fields attributed to the ministry they belong to, and this confirms that the work location does influence the study sample opinions towards the study fields.

CHAPTER (6)
CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

6.2 Conclusions

6.2.1 Information Security Management

6.2.2 Effectiveness of applying e-management

6.2.3 Correlations between the study fields

6.2.4 Differences among the study respondents' opinions

6.3 Recommendations

6.1 Introduction:

This chapter includes the most important conclusions which have addressed the impact of information security management on the effectiveness of applying e-management in the Governmental Institutions in Gaza. In addition, this chapter shows the proposed most important recommendations which may enhance information security management and e-management in the Palestinian Governmental Institutions.

6.2 Conclusions:

6.2.1 Information Security Management:

- The study revealed that the level of the overall fields of information security management was approximately (65.30%). On the other hand, there were clear weaknesses in some fields like: "*Personnel Security*", "*Organizational Security*", "*Compliance to Legal Requirements*" and "*Asset Classification and Control*".
- The study revealed that the level of Security Policy field was (66.30%).
- The study revealed that the level of Organizational Security field was (56.00%).
- The study revealed that the level of Asset Classification and Control field was (60.00%).
- The study revealed that the level of Personnel Security field was (53.40%).
- The study revealed that the level of Physical and Environmental Security field was (73.10%).
- The study revealed that the level of Computer and Network Management field was (69.30%).
- The study revealed that the level of System Access Control field was (74.70%).
- The study revealed that the level of Systems Development and Maintenance field was (73.40%).
- The study revealed that the level of Business Continuity Planning field was (69.90%).
- The study revealed that the level of Compliance to Legal Requirements field was (58.00%).

6.2.2 Effectiveness of applying e-management:

The study revealed that the level of the effectiveness of applying e-management in the Governmental Institutions in Gaza was (74.50%).

6.2.3 Correlations between the study fields:

- There is a significant statistical correlation at level ($\alpha = 0.05$) between the fields of information security management and the effectiveness of applying e-management in the Governmental Institutions in Gaza.

6.2.4 Differences among the study respondents' opinions:

- There are no significant statistical differences at level ($\alpha = 0.05$) among the respondents in their opinions about the study fields attributed to gender, age, level of qualification, specialization and the Governmental Institution.
- There are significant statistical differences at level ($\alpha = 0.05$) among the respondents in their opinions about the study fields attributed to experience and main work field.

6.3 Recommendations:

- Palestinian Government is advised to establish a written security policy with regards to the requirement of information security management.
- Palestinian Government should include information security theme in its strategic plans and consider the changeable environment and regularly review existed plans.
- Palestinian Government should enhance information security management departments and involve them in developing its strategies.
- Palestinian Government is advised to exert more efforts towards the organizational security field.
- Palestinian Government should obtain specialized information security advice where appropriate.

- The implementation of security policy should be reviewed independently on regular basis in order to provide assurance that organizational practices properly reflect the policy, and that it is feasible and effective.
- Palestinian Government should establish a cross-functional forum of management representatives from relevant parts of the institution to coordinate the implementation of information security controls.
- Palestinian Government should apply mechanisms to enable the evaluating and controlling the kinds and costs of security incidents and the potential damage.
- There should be founded an Information classification scheme or guideline in place; which will assist in determining how the information is to be handled and protected.
- All employees of the institution should receive appropriate Information Security training.
- Staff should be informed on the latest updates on the policies and procedures of an institution information security.
- Palestinian Government should establish a formal reporting procedure or guideline for users, to report security weakness in, or threats to, systems or services.
- Palestinian Government is advised to exert more efforts towards the personnel security field.
- Palestinian Government should further support its efforts towards the physical and environmental security field.
- Palestinian Government security policies should address software licensing issues such as prohibiting usage of unauthorized software.
- Operating plans should include incident management procedures to handle security incidents.
- Audit logs should be maintained for any change made to the operating programs.
- Some guidelines should be in place to guide users in selecting and maintaining secure passwords.
- A regular process should be available to review and evaluate user access rights and privileges.

- Strict control procedures should be in place over executing any changes to the information systems to minimize the corruption of them.
- Some controls should be in place for the execution of software on operating systems to minimize the risk of corrupting operating systems.
- Work continuity plans should be tested regularly to ensure that they are up to date and effective.
- All areas within the institution should be considered for regular review to ensure compliance with security policy, standards and procedures.
- Palestinian Government is advised to exert more efforts towards the compliance to legal requirements field.
- Palestinian Government is advised to improve and support its self-resources to ensure the continuity and development of applying the e-management on the strategic term.
- Personnel should take the needed training on technical tools according to their job needs.

References

Books

Araji, A., & Others. (1982). *Theories of management development* (First Edition ed.). Iraq: Ministry of Higher Education and Scientific Research.

Brealey, R., & Myers, S. (2000). *Principles of Corporate Finance.* New York: McGraw-Hill Companies .

Dhillon, G. (2001a). *Principles for managing information security in the new millennium. In G. Dhillon, Information security management: Global challenges in the new millennium.* London: Idea Group Publishing.

Ferrari, E., & Thuraisingham, B. (2006). *Web and information security.* Hershey, London: IRM Press.

Ghoneim, A. M. (2004). *E-management: present prospects and future aspirations.*

Ghorab, E. M. (2003). *E-learning, the entrance to the non-traditional training.* Arab Republic of Egypt, Cairo: Arab Organization for Administrative Development, Arab League.

Hussain, A. (2000). *Managing operational risk in financial markets.* Oxford: Butterworth Heinemann.

Najim, N. A. (2004). *E-management: the strategy, functions, and problems.* Riyadh: Almarekh Publishing House.

Pipkin, D. L. (2000). *Information security: protecting the global enterprise.* New Jersey: Prentice Hall PTR.

Popper, K. (1945). *The Open Society and Its Enemies.* London, United Kingdom: Routledge.

Salmi, A. A. (2003). *Information management systems.* Cairo: Arab Organization for Administrative Development.

Shawish, M. N. (2004). *Human Resources Management* (Third Edition ed.). Amman: Alshorouq House for publication and distribution.

Shimpi, P. (1999). *Integrating Corporate Risk Management.* New York: Texere LLC.

Steinkea, C. (2011). *Encyclopedia of Information Assurance: Physical Security* (DOI: 10.1081/E-EIA-120046881 ed.). U.S.A: Taylor & Francis.

Yassin, S. G. (2005). *E-management and its Arab applications' prospects.* Riyadh: Institute of Public Administration.

Jornal Articles

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security, 28*(6), 476-490.

Ashenden, D. (2008). Information security management: A human challenge? Information Security Technical Report, *ScienceDirect*, 13(4), 195-201.

Baker, S., Ponniah, D., & Smith, S. (1998). Techniques for the analysis of risk in major projects. *The journal of the operational research society, 49*(6), 567-572.

Basie, S. (2005). Information Security Governance - Compliance management vs operational management. Computers and Security, ELSEVIER, 24(6), 443-447.

Belsis, P., Kokolakis, S., & Kiountouzis, E. (2005). Information systems security from a knowledge management perspective, Information Management & Computer Security, 13(3), 189 – 202.

Botha, J., & Von Solms, R. (2004). A cyclic approach to business continuity planning. Information Management & Computer Security, 12(4), 328 – 337.

Chan, M., & Kwok, L. (2001). Integrating security design into the software development process for e-commerce systems. *Information Management & Computer Security, 9*(3), 112-122.

Gerber, M. (2001). Formalizing information security requirements. *Information Management & Computer Security, 9*(1), 32-37.

Grance, T., Hash, J., & Stevens, M. (2004). Security Considerations in the Information System Development Life Cycle. *NIST*.

Gritzalis, S., Iliadis, J., & Oikonomopoulos, S. (2000). Distributed component software security issues on deploying a secure electronic marketplace. *Information Management & Computer Security, 8*(1), 5-13.

Hong, K., Chi, Y., Chao, L., & Tang, J. (2003). An integrated system theory of information security management. *Information Management & Computer Security, 11*(5), 243-248.

Hutchinson , W., & Warren, M. (2001). Attitudes of Australian information system managers against online attackers. *Information Management & Computer Security, 9*(3), 106-111.

Irakleous, I. (2002). An experimental comparison of secret-based user authentication technologies. *Information Management & Computer Security, 10*(3), 100-108.

ISO/IEC 27001. (2005). *Information technology -- Security techniques -- Information security management systems – Requirements.* ISO/IEC 27001:2005 International Organization for Standardization and International Electrotechnical Commission.

ISO/IEC 27002. (2005). *Information technology -- Security techniques -- Code of practice for information security management. ISO/IEC 27002:2005.* International Organization for Standardization and International Electrotechnical Commission.

Janbandhu, P., & Siyal, M. (2001). Novel biometric digital signature for Internet-based applications. *Information Management & Computer Security, 9*(5), 205-212.

Knapp, K., & others. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security, 14*(1), 24-36.

Kwon, S., Jang, S., Lee, J., & Ki, S. (2007). Common defects in information security management system of Korean companies. *The Journal of Systems and Software, 8*, 1631-1638.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security, 10*(2), 57-63.

Loukis, E. (2001). Information systems security in the Greek public sector. *Information Management & Computer Security, 9*(1), 21-31.

Luthy, D., & Forcht, K. (2006). Laws and regulations affecting information management and frameworks for assessing compliance. *Information Management & Computer Security, 14*(2), 155-166.

Maguire, S. (2002). Identifying risks during information system development: managing the process. *Information Management & Computer Security, 10*(3), 126-134.

Morgan , G. (1996). Images of organization. *Thousand Oaks, CA: Sage Publications*.

Niekerk, J., & Solms, R. (2010). Information Security Culture: A management Perspective. *Computer and Security, ScienceDirect, ELSEVIER, 29*, 476-486.

Ozkan, S., & Karabacak, B. (2010). Collaborative risk method for information security management practices: A case context within Turkey. *International Journal of Information Management, 3*, 567–572.

Phukan, S. (2000). Ethics and information technology use: a survey of US based SMEs. *Information Management & Computer Security, 8*(5), 239-243.

Rhee, H., Ryn, Y., & Kim, C. (2012). Unrealistic optimism on information security management. *Computer and Security, ELSEVIER, 31*, 221-232.

Saleh, M. S., & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics, 9*, 107–118.

Seleznyov, A., & Puuronen, S. (2003). Using continuous user authentication to detect masqueraders. *Information Management & Computer Security, 11*(3), 139-145.

Shandu, R., Coyne, E., Feinstein, H., & Youman, C. (1996). Pole-based access control models. *IEEE Computer, 29*(2), 38-47.

Solms, B., & Solms, R. v. (2004). The 10 deadly sins of information security management. *Computers and security, ELSEVIER, 23*, 371-376.

Solms, R. (1998b). Information Security Management: the Code of Practice for Information Security Management (BS 7799). *Emerald, 6*(5), 224-225.

Solms, R. v. (1998a). Information security management: why information security is so important. *Emerald, 6*(4), 174-177.

Tsoumas, V., & Tryfonas, T. (2001). From risk analysis to effective security management: towards an automated approach. *Information Management & Computer Security, 12*(1), 91-101.

von Solms , B. (2001). Information Security — A multidimensional discipline. *Computers & Security, 20*(6), 504-508.

von Solms, B. (2000). Information security – the third wave? *Computers & Security, 19*(7), 615-620.

von Solms, B. (2006). Information Security – the Fourth Wave. *Computers & Security, 25*(3), 165-168.

von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security, 23*(5), 371-376.

Wangwe, C. K., Eloff, M. M., & Venter, L. (2012). A sustainable information security framework for e-Government – Case of TANZANIA. *Technological and economic development of economy, 18*(1), 117–131.

White, G., & Pearson, S. (2001). Controlling corporate e-mail, PC use and computer security. *Information Management & Computer Security, 9*(2), 88-92.

Ye, N. (2001). Robust intrusion tolerance in information systems. *Information Management & Computer Security, 9*(1), 38-43.

Yildirim, E. Y., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management, 3*(1), 360–365.

Thesis

A'l Dahwan, A. (2008). The role of the managerial development administration in applying e-management. *King Saud University*.

Al-Ajez, I. (2011). The role of organizational culture to activate the application of e-management. *Islamic University of Gaza*.

Al-Aloul, A. (2011). The available requirements for successful implementation of e-management at charitable associations in Gaza. *Islamic University of Gaza*.

Albrechtsen, E. (2008). Friend or foe? Information security management of employees. *Doctoral Thesis, Norwegian University of Science and Technology, Faculty of Social Sciences and Technology Management, Department of Industrial Economics and Technology Management*.

Aldafi, M. A. (2006). The possibility of the application of e-management in the General Directorate of Passports in Riyadh. *Unpublished Master's Thesis.* Riyadh: Naif University for Security Sciences.

Al-Ghoty, M. (2006). The requirements for successful implementation of e-Government at the Palestinian ministries. *Islamic University of Gaza*.

Al-Kubaisy, K. (2008). The requirements of applying e-management in the information systems center belonging to Quatar Government. *The International Virtual University*.

Al-Otaibi, O. (2010). The information security of websites and its compatibility with local and international standards. *Phd dissertation published at Prince Nayef Universty*.

Al-Somairy, M. (2009). The requirements of applying the e-management at the secondary schools in Gaza and the developing methods. *Islamic University of Gaza*.

Ammar, M. (2009). The possibility to apply electronic management in the United Nations Relief and Work Agency – Gaza Field Office. *Islamic University of Gaza*.

Brag, V., & Wedefelt, F. (2004). Information Risk Management- A case study of major Swedish Banks concerning the concept of Information Risk Management. *Business Administration - Industrial and Financial Management- Goteborg University*.

Frangopoulos, E. (2007). Social engineering and the ISO/IEC 17799:2005 security standard: a study on effectiveness. *Master of Science Thesis, School of Computing, University of South Africa*.

Goh, R. (2003). Information Security: The Importance of the Human Element. *Thesis for doctoral of philosophy in business administration - Faculty of the Preston University*.

Howard, J. D. (1997). An Analysis of Security Incidents on the Internet 1989 - 1995. *Ph.D. Thesis, Carnegie Mellon University*.

Mesfer, M. A. (2003). Administrative and practical obstacles to the use of computers in the security services. *Unpublished Master's Thesis.* Riyadh: Naif Arab University for Security Sciences.

Rastogi, R. (2011). Information Security Service Management - a service management approach to information security management. *Faculty of Engineering, Nelson Mandela Metropolitan University*.

Tayeh, A. (2008). Effectiveness of Information Security Management at the Palestinian Information Technology Companies. *Thesis, electronic version on Islamic University of Gaza website*.

Zoarob, F. (2009). The automation role in improving the performance of personnel affairs administration at the governmental ministries in Gaza. *Islamic University of Gaza*.

Conferences Proceedings, Reports and Surveys

AHTCC, AFP, & Others. (2006). Australian Computer Crime and Security Survey. Retrieved from http://www.auscert.org.au/render.html?it=2001

Ayoub, N. (2004). Electronic management. Second Administrative Forum. Riyadh: Saudi Management Association.

Eloff, J., & Eloff, M. (2003). Information security management - a new paradigm. *SAICSIT South African Institute for Computer Scientists and Information Technologists.* South Africa.

Endrei, M., Ang, J., Arsanjani, A., Chua, S., Comte, P., Krogdahl, P., et al. (2004). *Patterns: Services oriented architectures and web services.* IBM Redbook Series. http://www.redbooks.ibm.com/abstracts/SG246303.

Moss, J. (1998). *InternetWeek.*

OASIS. (2003b). *eXtensible access control markup language (XACML).* http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

Palestinian Central Bureau of Statistics. (2011). Retrieved from http://www.pcbs.gov.ps/default.aspx

Posthumus, S., & von Solms, R. (2005). A responsibility framework for information security. In Security Management, Integrity, and Internal Control in Information Systems. *Proceedings of the IFIP 11.1&11.5 Working Conference*, (pp. 205-221). Fairfax, Virginia, USA.

Radwan, R. (2004). E-management: management, and new global variables. *Second Administrative Forum for the Saudi Management Association.* Cairo: Information Center and Decision Support in the Council of Ministers.

Ranum, M. (1995). *USENIX security conference.*

SANS Institute. (1998). *NSA Glossary of Terms N SA Glossary of Terms Used in S ecurity and Intrusion Detection 1998.* http://www.sans.org/newlook/resources/glossary.htm.

Schlienger, T., & Teufel, S. (2002). Information security culture - The socio-cultural dimension in information security management. *In Proceedings of IFIP TC11 International Conference on Information Security (Sec2002): Security in the information society: visions and perspectives.*

Schultz, E. (1999). *Testimony befor congress.*

Sedukhin, I. (2003). *End-to-end security for web services and services oriented architectures.* http://whitepapers.interop.com/detail/RES/1066934613_132.html.

Singh, A. (2009). Improving Information Security Risk Management. *A Dissertation to the faculty of the graduate school of the Univeristy of Minnesota*.

Spafford, E. H. (1999). Reexamining intrusion detection. *University of Virginia.*

TechTV. (2001a). *'Cybercrime' Glossary.* http://www.techtv.com/cybercrime/aboutus/story/0,23008,3363041,00.html.

W3C .(2004) .*Web services architecture* .http://www.w3.org/TR/ws-arch./

Webopedia. (2002). *Webopedia Online Computer Dictionary.* http://www.webopedia.com.

Winn Schwartau .(1991) .*Testimony before Congress.*

Web sites

Fiedler, A. E. (2003). *The Standard ISO17799 as international basis*. Retrieved from On the necessity of management of information security: http://www.noweco.com/wp/wp_iso17799e.htm

Ministry of Telecommunication and Information Technology
http://www.gcc.gov.ps

The General Personnel Council
http://www.diwan.ps

IEEE
http://www.ieee.org

APPENDIX (A)

Questionnaire Arbitrators

No.	Name	Description
1	Dr. Yousef Bahar	Islamic University of Gaza
2	Dr. Sami Abou-Al-Ross	Islamic University of Gaza
3	Dr. Rushdy Wady	Islamic University of Gaza
4	Dr. Khalil Namrouty	Islamic University of Gaza
5	Dr. Samir Safi	Islamic University of Gaza
6	Eng. Khalid Dehleez	Islamic University of Gaza – Scientific Research Deanship
7	Dr. Bassam Abu Hamad	Al Quds University - Faculty of Public Health
8	Dr. Ayman Alyazori	Assistant Deputy Minister of Planning
9	Eng. Ismail Hamada	Ministry of Telecommunication and Information Technology
10	Eng. Rami Al-Ghamry	Council of Ministers
11	Rasheed Abu Jahjooh	Ministry of Higher Education – Planning Department

APPENDIX (B)
English Questionnaire

Islamic University of Gaza
Postgraduate Deanship
Faculty of Commerce
Master of Business Administration

Questionnaire No. ……..

Dear Sir/Madam

The researcher conducts a study on:

Information Security Management for Strategic and Effective Implementation of e-Management at the Governmental Institutions in Gaza

This is to complement the requirements for obtaining the master degree in business administration from the Islamic University of Gaza.

For this purpose, the researcher has developed this questionnaire - which is in your hands - to recognize the impact of information security management on the effectiveness of applying e-management in the Governmental Institutions in Gaza.

Whereas information security is the science that works to provide protection for information from the potential risks that threaten or attack it. That is by providing tools to protect information from internal and external risks. In addition, e-management concept is the switching to the electronic tools such as computer networks to achieve administrative processes throughout the organization and reduce dependence on paper-based procedures.

Given the importance of your opinion in this study, the researcher hopes in your serious and sincere cooperation for the success of this study through answering all the questions of this questionnaire carefully and objectively, where the answers should express your opinions. Note that the information contained in this questionnaire will be confidential and will only be used for research purposes only.

Thank you very much for your time

Researcher

Alaa Al-Deen A. Mohammed Hassan

Part One: General Information: put (√) on the correct checkbox.

1 . Ministry / Institution Name.

…… ……

2 . Qualification.

□ General Secondary and below □ Diploma

□ Bachelor □ Master □ Ph.D.

3 . Specialization.

□ Computer Engineering □ Computer Science □ Information Technology

□ Business Administration □ Other (please specify) .....

4 . Age.

□ Less than 30 □ 30 to less than 40 □ 40 to less than 50 □ 50 and older

5 . Gender.

□ Male □ Female

6 . Job Title.

□ General Director □ Director □ Chief Department □ Chief Branch □ Engineer

□ Software Developer □ Data Entry □ Administrative Assistant □ Secretary □ Other

.....

7 . Experience at Government Jobs.

……

8 . Main Work Field.

□ Institution Management, Planning and Strategies Development

□ Software Application Development □ Database Application Development

□ Computer Networks and Operating Systems □ Archiving and Information Management

□ Other (please specify) .....

Part Two: Information Security Fields:

Put the proper answer from (1) for the lowest acceptance degree about the question content through (10) for the highest acceptance degree.

Field (1) Security Policy		
No.	**Question**	**From: 1-10**
1	There exists an information security policy known to all the employees.	
2	The existed information security policy states the institution approach to manage information security.	
3	There is a known and defined responsible department for information security policy and its review, maintenance and upgrade.	
4	The maintenance and review process considers any new affecting changes like: significant security incidents, news risks, changes in organizational or technical infrastructure.	

Field (2) Organizational Security		
No.	**Question**	**From: 1-10**
1	There is a cross-functional forum of management representatives from relevant parts of the organization to coordinate the implementation of information security controls.	
2	Responsibilities for the protection of individual informatics assets and for carrying out specific security processes were clearly defined.	
3	Specialized information security advice is obtained where appropriate.	
4	The implementation of security policy is reviewed independently on regular basis. This is to provide assurance that organizational practices properly reflect the policy, and that it is feasible and effective.	

Field (3) Asset classification and control		
No.	**Question**	**From: 1-10**
1	The institution uses a data record file to identify the important assets associated with each information system	
2	There is an Information classification scheme or guideline in place; which will assist in determining how the information is to be handled and protected.	
3	An appropriate set of procedures are defined for information labeling and handling in accordance with the classification scheme adopted by the organization.	
4	There are existed applied mechanisms enabling the evaluating and controlling the kinds and costs of security incidents and the potential damage.	

Field (4) Personnel Security		
No.	**Question**	**From: 1-10**
1	Security roles and responsibilities as laid in Organization's information security policy are documented in the employee job description card.	
2	Employees are asked to sign confidentiality or nondisclosure agreement as a part of their initial terms and conditions of the employment.	
3	All employees of the organization receive appropriate Information Security training.	
4	Be informed with the staff on the latest updates on the policies and procedures of an organization's information security	

5	A formal reporting procedure exists, to report security incidents through appropriate management channels.	
6	A formal reporting procedure or guideline exists for users, to report security weakness in, or threats to, systems or services.	
7	There is a formal disciplinary process in place for employees who have violated organizational security policies and procedures.	

Field (5) Physical and Environmental Security		
No.	**Question**	**From: 1-10**
1	The rooms, which have the Information processing service, are locked or have lockable cabinets or safes.	
2	The information is only on need to know basis, which means there exists some security controls for third parties or for personnel working in secure area.	
3	The equipment is protected from power failures by using permanent power supplies such as multiple feeds, UPS, backup generator etc.	
4	The power and telecommunication cables carrying data or supporting information services are protected from interception or damage.	
5	The equipment is maintained as per the supplier's recommended service intervals and specifications.	
6	Disposal storage device containing sensitive information are physically destroyed.	
7	Automatic computer screen locking facility is enabled. This would lock the screen when the computer is left unattended for a period.	

Field (6) Computer and Network Management		
No.	**Question**	**From: 1-10**
1	The security policy has identified any operating procedures such as back-up, equipment maintenance etc.	
2	Audit logs are maintained for any change made to the operating programs.	
3	There is existed an Incident Management procedure to handle security incidents.	
4	Duties and responsibilities about systems and equipment are separated in order to reduce opportunities for unauthorized modification or misuse of information or services.	
5	The capacity demands are monitored and projections of future capacity requirements and equipment upgrades are made.	
6	System acceptance criteria are established for new information systems, upgrades and new versions and suitable tests were carried out prior to acceptance.	
7	The security policy addresses software licensing issues such as prohibiting usage of unauthorized software.	
8	Antivirus software is installed on the computers to check and remove any viruses from computers and media and this software signature is updated regularly.	
9	There is a policy in place for the acceptable use of electronic mail.	

Field (7) System Access Control		
No.	**Question**	**From: 1-10**
1	The access control policy does address the rules and rights for each user or a group of users.	
2	There exists a regular process to review and evaluate user access rights and privileges.	

3	There are some guidelines in place to guide users in selecting and maintaining secure passwords.	
4	A unique identifier is provided to every user (There are not public accounts used by more than one user).	
5	The sensitive systems are provided with isolated computing environment such as running on a dedicated computer, share resources only with trusted application systems.	
6	An audit logs recording security relevant events are produced and kept for an agreed period to assist in future investigations and access control monitoring.	

Field (8) Systems development and maintenance		
No.	**Question**	**From: 1-10**
1	The data input to application system is validated to ensure that it is correct and appropriate.	
2	The data output of application system is validated to ensure that the processing of stored information is correct and appropriate.	
3	Encryption techniques were used to protect the data.	
4	There are some controls in place for the execution of software on operating systems. This is to minimize the risk of corrupting operating systems.	
5	There are strict control procedures in place over executing any changes to the information systems to minimize the corruption of them.	

Field (9) Business Continuity Planning		
No.	**Question**	**From: 1-10**
1	There is a managed process in place for developing and maintaining work continuity throughout the organization.	
2	The events that could cause interruptions to work process were identified.	
3	Plans were developed to restore business operations within the required time frame following an interruption or failure to work process.	
4	Work continuity plans are tested regularly to ensure that they are up to date and effective.	

Field (10) Compliance to Legal Requirements		
No.	**Question**	**From: 1-10**
1	All relevant statutory, regulatory and contractual requirements were explicitly defined and documented for each information system.	
2	Specific controls and individual responsibilities to meet these requirements were defined and documented.	
3	There exist and well implemented some procedures to ensure compliance with legal restrictions on use of material in respect of which there may be intellectual property rights (copyright, design rights, trade marks).	
4	All areas within the organization are considered for regular review to ensure compliance with security policy, standards and procedures.	

Part Three: Effectiveness of Applying e-Management:

Put the proper answer from (1) for the lowest acceptance degree about the question content through (10) for the highest acceptance degree.

Part (3) Effectiveness of Applying e-Management E-management concept is the switching to the electronic tools such as computer networks to achieve administrative processes throughout the organization and reduce dependence on paper-based procedures.		
No.	**Question**	**From: 1-10**
1	The top management supports applying the e-management at the institution.	
2	There is a special and appropriate team in place to apply e-management at the institution.	
3	The personnel accept the implementation of the e-management at the institution.	
4	The personnel have the appropriate knowledge and experience to deal with applying the e-management.	
5	The personnel take the needed training on technical tools according to their job needs.	
6	The internal administration procedures are done simply without any sophistication.	
7	The procedures to serve the out of institution stakeholders are done simply and without any sophistication.	
8	There are self-resources in place to ensure the continuity and development of applying the e-management at the strategic term.	
9	The institution stakeholders accept to deal with the institution via its internet website.	
10	There exist at the institution a lot of the technical requirements like (computers, network, server, hard disks, internet, software and systems)	
11	The software applications deliver the sufficient and accurate information properly.	
12	The e-management creates a secure environment to exchange information.	
13	There exists an effective system to define the authorized users to access the computerized information.	
14	The information back-up copies are kept in safe places out the institution.	
15	There exist clear and black policies for the personnel who violate the information confidentiality and security.	

APPENDIX (C)
Arabic Questionnaire

الجامعة الإسلامية غزة
عمادة الدراسات العليا
كلية التجارة
إدارة الأعمال

رقم الاستبانة : .....

الأخوة / الأخوات العاملون في المؤسسة الحكومية حفظكم الله ورعاكم،،،

السلام عليكم ورحمة الله وبركاته ،،،

يقوم الباحث بإجراء دراسة حول:

إدارة أمن المعلومات كمدخل استراتيجي لفاعلية تطبيق الإدارة الإلكترونية في المؤسسات الحكومية العاملة في محافظات غزة

وذلك استكمالاً لمتطلبات الحصول على درجة الماجستير في إدارة الأعمال من الجامعة الإسلامية – غزة.
ولهذا الغرض قام الباحث ببناء هذه الاستبانة – التي بين أيديكم– لمعرفة متطلبات تطبيق إدارة أمن المعلومات في المؤسسات الحكومية العاملة في محافظات غزة، وأثرها على فاعلية تطبيق الإدارة الإلكترونية فيها.

حيث أن أمن المعلومات هو العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية والخارجية، كما أن الإدارة الإلكترونية بمفهومها البسيط هي التحول إلى استخدام الوسائل الإلكترونية مثل الحاسوب والشبكات في إنجاز العمليات الإدارية الداخلية والخارجية للمؤسسة وتقليص الاعتماد على الإجراءات الورقية.

ونظراً لأهمية رأيكم في هذا الدراسة، يرجو الباحث تعاونكم الجاد والصادق لإنجاح هذه الدراسة من خلال التكرم بالإجابة عن جميع فقرات الاستبانة بدقة وعناية وموضوعية وأن تكون الإجابة معبرة عن آرائكم، علماً بأن المعلومات الواردة في هذه الاستبانة ستحظى بالسرية التامة ولن تستخدم إلَّا لأغراض البحث العلمي فقط.

وشكراً جزيلاً على وقتك

الباحث

علاء الدين عوض محمد حسن

القسم الأول: البيانات التعريفية: ضع علامة (√) في مربع الإجابة الصحيحة.

1. **اسم المؤسسة/ الوزارة.**

....

2. **المؤهل العلمي.**

□ ثانوية عامة فما دون □ دبلوم متوسط

□ بكالوريوس □ ماجستير □ دكتوراة

3. **التخصص.**

□ هندسة حاسوب □ علوم حاسوب □ تكنولوجيا معلومات □ إدارة أعمال □ غير ذلك (الرجاء التحديد)

.....

4. **العمر.**

□ أقل من 30 سنة □ من 30 إلى أقل من 40 سنة □ من 40 إلى أقل من 50 سنة □ 50 سنة فأكثر

5. **الجنس.**

□ ذكر □ أنثى

6. **المسمى الوظيفي** (اختر إجابة واحدة فقط من فضلك).

□ مدير عام □ مدير دائرة □ رئيس قسم □ رئيس شعبة

□ مهندس □ مبرمج □ مدخل بيانات □ موظف إداري □ سكرتير □ غير ذلك (الرجاء التحديد)

.....

7. **سنوات الخدمة في العمل الحكومي** (اكتب عدد سنوات الخدمة في العمل الحكومي من فضلك).

.....

8. **المجال الرئيسي لطبيعة العمل.**

□ إدارة المؤسسة ورسم الخطط والسياسات والاستراتيجيات □ تطوير التطبيقات البرمجية

□ تطوير تطبيقات قواعد البيانات □ نظم التشغيل والشبكات □ الأرشفة وحفظ المعلومات

□ غير ذلك (الرجاء التحديد) .....

القسم الثاني: مجالات إدارة أمن المعلومات.

ضع الدرجة المناسبة من درجة (1) الأقل موافقة على ما ورد في العبارة إلى درجة (10) الأكثر موافقة على ما ورد في العبارة.

المجال الأول: سياسة الأمن Security Policy		
م.	**السؤال**	**من 1 – 10**
1.	يوجد في المؤسسة سياسة لأمن المعلومات يعرفها جميع الموظفين.	
2.	سياسة أمن المعلومات الموجودة تبين طريقة المؤسسة في إدارة أمن المعلومات.	

.3	هناك جهة محددة ومعروفة مسؤولة عن سياسة أمن المعلومات ومراجعتها وتحديثها في المؤسسة.	
.4	تأخذ عملية المراجعة بعين الاعتبار الاستجابة لأية تغيرات جديدة (مثال: حوادث أمن مهمة أو مخاطر جديدة أو تغيرات على البنية التحتية الفنية أو التنظيمية).	

المجال الثاني: الأمن التنظيمي Organizational Security		
م.	**السؤال**	**من 1 – 10**
.1	يوجد في المؤسسة فريق (مكون من أفراد ممثلين لمعظم دوائر المؤسسة) مسؤول عن إدارة أمن المعلومات.	
.2	مسؤوليات حماية ممتلكات الأفراد المعلوماتية وتنفيذ عمليات إدارة أمن المعلومات واضحة ومحددة.	
.3	تقوم المؤسسة بالاستعانة بخبراء للحصول على استشارات في أمن المعلومات.	
.4	يتم تقييم تنفيذ سياسة الأمن من قبل جهة مستقلة للتأكد أن المؤسسة تمارس السياسة بشكل جيد وأن هذه السياسة ذات جدوى وفعالية.	

المجال الثالث: تصنيف الأصول (الممتلكات) وضبطها Asset classification and control		
م.	**السؤال**	**من 1 – 10**
.1	تستخدم المؤسسة سجلاً لحفظ بيانات الأصول (الممتلكات) ذات العلاقة بكل نظام من أنظمة المعلومات. (يبين السجل مستخدم ذلك الأصل ومكان وجوده).	
.2	يوجد جدول أو دليل تصنيف للمعلومات من شأنه أن يساعد في تحديد الكيفية التي يتم التعامل بها مع المعلومات وحمايتها.	
.3	يوجد مجموعة من الإجراءات المناسبة لعنونة المعلومات والتعامل معها طبقاً لجدول التصنيف.	
.4	يوجد آليات مطبقة تمكن من متابعة وتقدير أنواع وأحجام وتكاليف حوادث الأمن والتلف الذي تحدثه.	

المجال الرابع: الأفراد وأمن المعلومات Personnel Security		
م.	**السؤال**	**من 1 – 10**
.1	تحتوي وثيقة الوصف الوظيفي للموظف على مسؤولياته ومهامه تجاه أمن المعلومات في المؤسسة.	
.2	يتم الطلب من الموظفين التوقيع على تعهد بعدم الإفصاح عن معلومات المؤسسة كجزء من شروط توظيفهم.	
.3	يتلقى جميع الموظفين تدريباً مناسباً خاصاً بأمن المعلومات.	
.4	يتم إطلاع الموظفين على آخر التحديثات على سياسات وإجراءات أمن المعلومات في المؤسسة.	
.5	تتبع المؤسسة إجراءات رسمية لرفع التقارير بحوادث الأمن في المؤسسة من خلال القنوات الإدارية المناسبة.	
.6	يوجد إجراء رسمي يتبعه المستخدمون لرفع التقارير بمواطن الضعف والمخاطر الأمنية في الأنظمة والخدمات.	
.7	يتم تطبيق إجراءات تأديبية رسمية على الموظفين الذين ينتهكون إجراءات وسياسات أمن المعلومات في المؤسسة.	

المجال الخامس: الأمن المكاني Physical and Environmental Security		
م.	السؤال	من 1 – 10
.1	الغرف التي تحتوي على الأجهزة والمعلومات تكون مغلقة أو بها خزانات آمنة يمكن إغلاقها.	
.2	المعلومات متاحة فقط على أساس الحاجة إليها، بمعنى أنه يوجد ضوابط تحكم دخول الأفراد الخارجيين والأفراد الذين يعملون في مناطق آمنة.	
.3	الأجهزة محمية من انقطاع الكهرباء، بمعنى أنه يوجد في المؤسسة مولد كهرباء احتياطي، أو UPS ، أو أكثر من خط كهرباء.	
.4	كوابل الكهرباء والاتصالات التي تحمل البيانات أو تدعم خدمات المعلومات محمية من العبث بها أو إتلافها.	
.5	يتم عمل صيانة للمعدات بناءً على توصيات ونصائح المزود من حيث المواصفات والمواعيد.	
.6	يتم التخلص جيداً من أجهزة حفظ البيانات التي تحتوي على بيانات حساسة وتتعطل أو تصبح لا لزوم لها وذلك بإتلافها.	
.7	يتم تأمين شاشة الحاسوب بشكل يدوي أو آلي عند عدم استخدامها لفترة ما.	

المجال السادس :إدارة الشبكة والحواسيب Computer and Network Management		
م.	السؤال	من 1 – 10
.1	سياسة الأمن تحدد إجراءات التشغيل مثل النسخ الاحتياطي وصيانة الأجهزة وغير ذلك.	
.2	يتم استخدام سجلات تدقيق لأية تغيرات تتم على الأنظمة العاملة في المؤسسة.	
.3	يوجد إجراء إدارة الأحداث للتعامل مع أحداث أمن المعلومات.	
.4	المهام ونطاق المسؤوليات عن الأجهزة والأنظمة منفصلة وذلك من أجل تقليل فرص إجراء تغييرات غير مسموح بها أو منعاً لإساءة الاستخدام.	
.5	يتم متابعة احتياجات الأجهزة، وعمل توقع لمتطلباتها المستقبلية وسبل تطويرها.	
.6	هناك معايير لقبول أية أنظمة جديدة أو أية تعديلات أو نسخ جديدة من البرامج والأنظمة، ويتم إجراء اختبارات عليها قبل القبول بها.	
.7	تبين سياسة الأمن أموراً ذات علاقة بترخيص البرامج، مثل منع استخدام برامج غير مرخصة.	
.8	يتم استخدام برامج لمراقبة مكافحة وإزالة الفيروسات ويتم تحديث هذه البرامج باستمرار.	
.9	يوجد سياسة خاصة بالاستخدام المقبول للبريد الإلكتروني.	

المجال السابع: ضبط الوصول للأنظمة System Access Control		
م.	السؤال	من 1 – 10
.1	تبين سياسة ضبط الوصول القواعد والصلاحيات لكل مستخدم أو مجموعة من المستخدمين.	
.2	يوجد عملية دورية لمراجعة صلاحيات المستخدمين في الوصول للأنظمة.	
.3	يوجد توجيهات مطبقة لإرشاد المستخدمين في اختيار كلمات المرور والمحافظة عليها.	

.4	يوجد حساب (اسم مستخدم / وكلمة مرور) خاص لكل مستخدم، بمعنى أنه لا يتم استخدام حسابات عامة يستخدمها أكثر من شخص.	
.5	يتم عزل الأنظمة الحساسة في بيئة عمل منفصلة، مثلاً أن تكون على جهاز مستقل وتتشارك المصادر فقط مع الأنظمة الموثوقة.	
.6	يتم استخدام سجلات متابعة لحفظ أحداث ذات علاقة بالأمن، ويتم الاحتفاظ بها لفترة زمنية متعارف عليها، وذلك للمساعدة في أية تحقيقات مستقبلية.	

المجال الثامن: تطوير وصيانة الأنظمة Systems development and maintenance		
م.	**السؤال**	**من 1 – 10**
.1	يتم التحقق من صحة البيانات المدخلة للأنظمة للتأكد أنها صحيحة ومناسبة.	
.2	يتم التحقق من المخرجات الناتجة من الأنظمة للتأكد أن معالجة المعلومات المخزنة تمت بشكل صحيح.	
.3	يتم استخدام آليات تشفير لحماية البيانات.	
.4	يوجد ضوابط مطبقة على تنفيذ البرامج على أنظمة التشغيل، وذلك بهدف تقليل مخاطر تعرض أنظمة التشغيل للتلف.	
.5	يوجد إجراءات ضبط صارمة مطبقة على تنفيذ أية تغييرات على أنظمة المعلومات، وذلك لحمايتها من العطل.	

المجال التاسع: تخطيط استمرارية العمل Business Continuity Planning		
م.	**السؤال**	**من 1 – 10**
.1	يتم في المؤسسة تطوير واستخدام خطة لاستمرارية العمل.	
.2	تم تحديد وتعريف الأحداث التي قد تؤدي إلى توقف العمل.	
.3	يوجد خطة لإعادة الأعمال إلى طبيعتها ضمن الإطار الزمني المطلوب بعد حدوث إخفاق أو انقطاع في أداء العمل.	
.4	يتم اختبار خطط استمرارية العمل بشكل دوري للتأكد من أنها محدثة وفعالة.	

المجال العاشر: الامتثال للمتطلبات القانونية Compliance		
م.	**السؤال**	**من 1 – 10**
.1	تم تحديد وتوثيق المتطلبات القانونية والتنظيمية والتعاقدية ذات العلاقة بكل نظام معلومات.	
.2	تم تحديد وتوثيق الضوابط والمسؤوليات الفردية لتلبية تلك المتطلبات.	
.3	يوجد إجراءات للتأكد من الامتثال للقيود القانونية في استخدام المواد التي قد يكون لها حقوق ملكية فكرية، مثل حقوق الطبع والتصميم والعلامات التجارية.	
.4	يتم عمل مراجعة دورية لجميع أجزاء المؤسسة للتأكد من الامتثال لسياسة الأمن والإجراءات والمعايير.	

القسم الثالث: مستوى فاعلية تطبيق الإدارة الإلكترونية.

ضع الدرجة المناسبة من درجة (1) الأقل موافقة على ما ورد في العبارة إلى درجة (10) الأكثر موافقة على ما ورد في العبارة.

مستوى فاعلية تطبيق الإدارة الإلكترونية الإدارة الإلكترونية بمفهومها البسيط هي التحول إلى استخدام الوسائل الإلكترونية مثل الحاسوب والشبكات في إنجاز العمليات الإدارية الداخلية والخارجية للمؤسسة وتقليص الاعتماد على الإجراءات الورقية.		
م.	**السؤال**	**من 1 – 10**
.1	تدعم الإدارة العليا تطبيق الإدارة الإلكترونية في المؤسسة.	
.2	يتوفر لدى المؤسسة فريق مناسب متخصص لتطبيق الإدارة الإلكترونية.	
.3	يتقبل العاملون تطبيق الإدارة الإلكترونية في المؤسسة.	
.4	يتوفر لدى العاملين معرفة وخبرة مناسبة للتعامل مع بيئة الإدارة الإلكترونية.	
.5	يتم تدريب العاملين على الوسائل التقنية بناءً على احتياجاتهم الوظيفية.	
.6	تتم الإجراءات الإدارية الداخلية ببساطة وبدون تعقيدات.	
.7	تتم إجراءات تقديم الخدمة للمستفيدين من خارج المؤسسة ببساطة وبدون تعقيدات.	
.8	يوجد لدى المؤسسة موارد ذاتية لضمان استمرار وتطوير الإدارة الإلكترونية على المدى الاستراتيجي.	
.9	يوجد قبول واستعداد من المستفيدين من خدمات المؤسسة للتعامل معها من خلال الموقع الإلكتروني للمؤسسة.	
.10	يتوفر لدى المؤسسة معظم المتطلبات التقنية مثل (أجهزة حاسوب، شبكة حاسوب، سيرفر، وسائل تخزين البيانات، إنترنت، الأنظمة والبرامج) لتطبيق الإدارة الإلكترونية.	
.11	توفر البرامج المعلومات بالكمية والدقة المناسبتين.	
.12	توفر الإدارة الإلكترونية بيئة آمنة لتبادل المعلومات.	
.13	يتوفر لدى المؤسسة نظام فاعل لتحديد الأشخاص المخولين للوصول إلى المعلومات المحوسبة.	
.14	يتم الاحتفاظ بنسخ احتياطية من البيانات في أماكن آمنة خارج المؤسسة.	
.15	تتوفر سياسات واضحة ورادعة للموظفين الذين ينتهكون أمن وسرية المعلومات.	