The Islamic University-Gaza
Higher Education Deanship
Faculty of Commerce
Business Administration Dept.

Information Security and Communications Management in light of Networks Technology

"Case study: Islamic University of Gaza"

Submitted By
Raed J. Altoom

Supervised By
Prof. Dr. Yousif Hussain Ashour

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTSFOR THE DEGREE OF MBA

May , 2013

ABSTRACT

The security of information and communication is considered as one of important areas these days and plays a significant role in protecting, preserving and fortifying security systems in all institutions and particularly at the Islamic University – Gaza (IUG).

The research aims to manage the security of information and communication technology (ICT) systems in light of the networks within the IUG. The research used the analytical descriptive approach and the comprehensive survey to introduce the research data in order to meet research objectives using the Statistical Package for the Social Sciences (SPSS). 72 questionnaires were distributed as a tool in survey the opinions of the research population, the collected questionnaires were (56) representing response rate (78%).

The research concluded that there is a statistically significant relationship between the risks of the surrounding technology and systems security level according to of the population point of view that associated with natural disasters such as turning off the energy sources , fires and intentional disasters such as the Israeli attack on the infrastructure of information and communication technology (ICT). The study recommended to find a suitable alternative to manage and control the safety of the information system in and out the IUG to maintain the integrity of information, and the development of policies and procedures to protect the security information systems in the IUG, staff training on the latest technologies information by joining international conferences, learning from other experiences worldwide in addition to the commitment of senior management in the IUG in order to support the security information systems.

إدارة أمن المعلومات والإتصالات في ضوء تكنولوجيا الشبكات

دراسة حالة على الجامعة الإسلامية– بغزة

الملخص

إن إدارة أمن المعلومات والاتصالات تعتبر أحد المجالات الهامة هذا العصر، وتلعب دوراً هاما في حماية وصون وعدم اختراق الأنظمة في جميع المؤسسات، وخاصة في "الجامعة الإسلامية.

هدفت هذه الدراسة إلى دراسة إدارة امن المعلومات والاتصالات في ضوء تكنولوجيا الشبكات في الجامعة الإسلامية في غزة. ولقد تم استخدام المنهج الوصفي التحليلي ، وتم استخدام والمسح الشامل لمجتمع الدراسة لجمع البيانات من أجل تلبية أهداف البحث، وباستخدام (SPSS) تم توزيع (72) استبانه لاستكشاف آراء مجتمع الدراسة، كانت الاستبيانات التي تم جمعها (56) تمثل نسبة الاستجابة (78٪). وبعد إجراء عملية التحليل لبيانات الدراسة وفرضياتها توصلت الدراسة إلى عدد من النتائج وكان أهمها: أن هناك علاقة ذات دلالة إحصائية بين مخاطر التكنولوجيا المحيطة ومستوى إدارة أمن النظام من وجهة نظر عينة الدراسة المرتبطة بالكوارث الطبيعية مثل انقطاع مصادر الطاقة والحرائق، والكوارث المتعمدة مثل الهجوم الإسرائيلي علي البنية التحتية الأساسية لتكنولوجيا المعلومات والاتصالات، لذا توصي الدراسة لإيجاد البديل المناسب والعمل علي إدارة و مراقبة و حفظ نظام

المعلومات التي تتم من داخل و خارج الجامعة للحفاظ على سرية المعلومات، ووضع السياسات والإجراءات لحماية أمن نظم المعلومات في الجامعة الإسلامية بغزة، كما وتدريب الموظفين على أحدث تقنيات تكنولوجيا المعلومات من خلال الانضمام إلى المؤتمرات الدولية والتعلم من التجارب الأخرى في جميع أنحاء العالم والتزام الإدارة العليا في الجامعة الإسلامية بدعم أمن نظم المعلومات بشكل مستمر.

DEDICATION

I would like to take this opportunity to express my deepest thanks and lovingly dedicate this work to: my parents, wife, sons, brothers, sisters and friends. They have given me the drive and discipline to tackle any task with enthusiasm and determination,

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. Yousif H. Ashour 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; Dr Issam Al-Buhaisi and Dr Samy Abu Naser, for their cordial support, valuable information and guidance, which helped me in completing this task through various stages.

Lastly, I would like to thank all people who helped me in completing this work.

Eng. Raed J. R Altoom

May-2013

Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

(CIA) Confidentiality, Integrity And Availability

(CTO) Chief Technology Officer

(CSI/FBI) Computer Security Institute/Federal Bureau of Investigation

(ICTs) Information and Communication Technologies

(ISMS) Information Security Management System

(ISO) International Organization for Standardization

(ISRM) Information Security Risk Management

(IUG) Islamic University of GAZA

(KM) Knowledge Management

(OSI) Open Systems Interconnection

(SPSS) Statistical Package for the Social Sciences

CHAPTER 1:GENERAL INTRODUCTION

First: Background

Second: research problems

Third: Research variables

Fourth: Research hypotheses

Fifth: Research objectives

Sixth: Research importance

Seventh: Research approach and methodology

Eighth: Previous studies

Ninth: The Previous studies discussion

First: Background

Information and Communication Technologies (ICTs) play an essential role in the field of education. ICT deals with the application of different electronic media in collection, storage, and rapid access of information to users. Its benefits reach everyone in the niche and corner of the world. The basic elements of ICT are communication, storage and retrieval of knowledge. Libraries, besides the repositories of books and journals, now become access points for data bases, websites and a range IT-based products. ICT stimulates the learners to acquire quality research through team work and time management. New technologies namely satellite communication, Fiber Optic cable and computers have enhanced educational capabilities .ICT has certainly improved our lives. It can be best harnessed to improve the efficiency and effectiveness of education at all levels in both formal and non-formal settings. (Swaminathan and Sekar:2012).

information technology is widely recognized as the engine that drives the U.S. economy, giving industry a competitive advantage in global markets, enabling the federal government to provide better services to its citizens, and facilitating greater productivity as a nation. Organizations in the public and private sectors depend on technology-intensive information systems to successfully carry out their missions and business functions. Information systems can include diverse entities ranging from high-end supercomputers, workstations, personal computers, cellular telephones, and personal digital assistants to very specialized systems. Information systems are subject to serious threats that can have adverse effects on organizational operations (i.e., missions, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation by exploiting both known and

unknown vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems. Threats to information and information systems can include purposeful attacks, environmental disruptions, and human/machine errors and result in great harm to the national and economic security interests of the United States. Therefore, it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk - that is, the risk associated with the operation and use of information systems that support the missions and business functions of their organizations.(National Institute of Standards and Technology Gaithersburg:2011)

Due to fast pace of change in ICT technology and its important applications, new security threats revolve around it. New and smart methods of information security are also devised by researchers to mitigate the risk occurred due to these threats. In the last decade process based information security management system(ISMS) such as ISO27001 and COBIT have emerged. Many organizations since then have adopted such ISMS. Knowledge Management(KM) is another management discipline enterprises employ, with aim to foster a more effective management of knowledge (Richard Y. K. Fung, 2008).

(IUG) makes use of information technology and communications (ICT), for instance, all the administrative, educational and registration issues are computerized through public networks. As shown in Table(1.1) in 2013,the number of registered students is 19241, while the number of the academic and administrative staff is 876 employee. The number of offered courses for the whole faculties is 1186.

Table no. (1.1): The number of academic, students and administrative staff of the IUG

university staff	Numbers
Academics	413
administrator	463
Students	19,241
Total	20,117

(According to the department of registration of the IUG)

Thus it becomes necessary to manage and protect the information. The network in IUG has like most of the communication networks weak access such as, the illegal use of the database information by students and employees. The separation between tasks and mandates of the employers. Moreover, it happened many time that, hackers penetrate the system….etc. Therefore, this research is concentrated for managing the security of information and communication in the network Technology in IUG. It becomes great interest providing necessary methods to protect information systems, control over their processes, ensure the sustainability of these systems correctly and in the required manner what it has been.

Second: Problem of Research

The IUG experience in using the information technology in its systems communication internally and externally and securing high level of security to its networks from theft and illegal penetration, but in parallel the number of attacks and hackers to the IUG network are increasing. As it is well known, the security information and communication management is affected by many factors .

The research question : what are the factors that influence the management of information security and communications at the IUG **?**

Third: Research variables

1. Dependent variable:

The security of information and communication management

2. Independent variables:

The research independent variables including the following:

a) Risks of input data

b) Risks of output data

c) Surrounding Technology

d) Lack of experience and training

e) Weakness of control procedure

f) Policies and procedures

Fourth: Research hypotheses

Main Hypothesis (1):

There is a statistically significant effect at (α=0.05) of the security information and communication management factors on the security of information and communication management

Sub-hypothesis:

H1a: There is statistically significant effect at (α=0.05) of risks input data on the security of information and communication management.

.**H1b:**There is statistically significant effect at (α=0.05) of risks output data on The security of information and communication management.

H1c: There is a statistically significant effect at (α=0.05) of surrounding on The security of information and communication management.

H1d: There is a statistically significant effect at (α=0.05) of lack experience and training on the security of information and communication management.

H1e: There is statistically significant effect at (α=0.05) of weakness of control procedure on the security of information and communication management.

H1f: There is a statistically significant effect at (α=0.05) of policies and procedures on the security of information and communication management

Main Hypothesis (2):

H1: There is a significant difference among the respondents' toward (Information Security and Communications Management in light of Networks Technology) due to demographic characters (gender, age, experience, job title, qualifications).

Fifth: Research objectives

The main goal of current research is to manage information and communication security in light of network technology at the (IUG), through the following objectives:

1. Determine the impacts of the input data risks on the security of information and communications in IUG.
2. Determine the impacts of the output data risks on the security of information and communications in IUG.
3. Determine the impacts of surrounding technology risks on the security of information and communications in IUG.
4. Determine the impacts of lack experience and training risks on the security of information and communications IUG
5. Determine the impacts of weakness of control procedure risks on the security of information and communications IUG
6. Determine the impacts of policies and procedures on information security and communications in IUG
7. To suggest recommendations that might help IUG in improving the security of information system in communications and networks technology.

Sixth: The importance of research

The importance of the current research comes from the following points.

1. This research interpreted modern and rapid developed technology, whereas any misleading results will lead to serious and high risk especially it concerns the information and networks management at the IUG.
2. Highlight most risks related to the inputs and outputs of the PC and the control procedures for systems at IUG.
3. Highlight the surrounding technology risks due to the human mistakes in the IUG and proposed procedures to limit that risks at IUG.
4. The need of the IUG to such research to minimize the risks of repeated penetrations and thefts through the system management to ensure the confidence of it.
5. The current research is a simple reference for any proposed research for the system at the IUG.

Seventh: Research approach and methodology

The methodology of this research is as follows

1. The study follows the procedure of a descriptive study. The researcher adapted analytical approach which depends on data collection, analysis using SPSS and interpretation of the results to determine the hypothesized relationships. The questionnaire was conduct to reach the result of the study

a) **Primary Data:** The research used the analytical descriptive approach and the comprehensive survey to introduce the research data in order to meet research objectives using the Statistical Package for the Social Sciences (SPSS). 72 questionnaires were distributed as a tool in survey the opinions of the research population, the collected questionnaires were (56) representing response rate (78%).

b) **Secondary Data:** This research depended on published and unpublished material such as referred journals, papers, text books and internal resources.

2. Questionnaire to ensure the proposed hypothesis, the target group were directors of the departments , heads of sections and all the staff of the information technology department.

Eighth: Previous studies

First: Arabic Studies:

1. **Alaa Al-Deen,(2013):Information Security Management for Strategic and Effective Implementation of e-Management in the Governmental Institutions in Gaza**

This research aimed to identify the impact of information security management on the effectiveness of applying e-management in the Governmental Organizations in Gaza. The 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 research found that 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 research recommend that 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.

2. **Obeidi, Hadeel Shawkat (2010): Security of information and communication technology: a research of user awareness in the Kingdom of Bahrain.**

This research aimed to the security of the information and communication technology at the level of users and the strategies to be followed in their organizations.

In addition to displaying some of the proposed solutions to measure the degree of awareness of users and areas of those solutions.

The research found that there are a lot of risks that diminish the security of information and communication technology in the institutions operating in the State of Bahrain.

In addition to that there are many solutions that enable organizations to maintain the confidentiality of information, including, encryption and firewall.

3. **Badi, Walid Salem (2010): The reality of information systems security in the Omani libraries: a case research on the main library at Sultan Qaboos University.**

This paper aimed to recognize the reality of the security of information systems in Oman libraries through the assessment of the reality of information systems security library Sultan Qaboos University.

The results of the research are lack of central oversight responsibility for security on automated systems.

It required clear policy for the mechanism of information and communication systems to deal with some of the risks and anticipated threats such as libraries penetration and building a virtual database means to transfer all the data to the real basis for the library system.

4. **Zidane&Hamo (2010): Banking information security requirements in the Internet Technology.**

This paper proposes the requirements of achieving information security to the banks in the online Technology and ways of confronting banking fraud.

Highlighting the efforts of the public banks in the Kingdom of Saudi Arabia in the face of piracy informatics.

The research found the presence of IT global infrastructure used by financial institutions and banks that would ensure security and safety of the work of these institutions,

There is a development in the field of IT security information to deal with security threats related to the Internet. There is a lack of legislation and laws regulating the banking business in the Technology Internet. The absence of standards and principles for screening and the query, which leads to the occurrence of financial and banking fraud.

Second: foreign studies:

5. **Swaminathan, P. Sekar, (2012):Information and Communication Technology (ICT) and Society.**

This paper illustrated the Information and Communication Technology (ICT) has certainly improved our lives.

It can be best harnessed to improve the efficiency and effectiveness of education at all levels in both formal and non-formal settings.

It has made our material life easier and happier. But it has brought new forms of national and international issues of ethics and human values in the mask of Globalization. It has a potential threat to the valuable aspects of our ancient culture and traditions.

The goal of this paper It has potentially powerful tools for effecting reforms and lifestyle. It paves way for a new system of teaching and learning process.

6. **George SUCIU, V. POENARU, (2011) : A Research of Implementing an Information Security Management System for Open Source Cloud Computing.**

This article illustrates that An Information Security Management System (ISMS) contains a coordinated set of activities, processes, controls, and policies with the purpose of protecting and managing the information assets within an organization.

In this paper we present the way in which an ISMS as specified in the ISO 27001 can be applied for the cloud and implemented on our test platform based on SlapOS, the first open source provisioning and billing system for distributed cloud computing.

The goal of this paper is to demonstrate a new and easier way to manage security for the cloud, with a specific focus on distributed cloud computing. they will present the results measured by applying ISMS controls for ensuring levels of QoS and SLA according to contracts, moreover also optimizing the costs and resources used by the cloud platform.

Threats and vulnerabilities regarding information security are pushing organizations to better protect their valuable information and resources by using an information security management system.

7. **Takemura , (2010):Quantitative Research on Japanese Workers' Awareness to Information Security Using the Data Collected by Web-Based Survey.**

This research aimed that The researches in the field of social sciences such as economics and business management were not conducted until around 2000. Particularly, there are few empirical studies on information security. Primary reasons among various ones are that there is no data on information security countermeasures and we cannot easily use the data even if the data exist. Though it is in such a research environment, it is necessary to accumulate the research from not only promotion of academic research but also the social role. In this research, the author quantitatively analyzed Japanese workers awareness to information security.

The author examined whether or not there are differences of the workers' awareness to information security based on various attributes by using Analysis Of Variance (ANOVA) based on non-parametric method.

It is found that Japanese workers awareness to information security is different in attributes such as organizational attributes and the education about information security countermeasures.

The author suggested the necessity of enhancing information security education and introducing firm system such as authority handover system and/or stock option system in order to motivate to take the efficient information security countermeasures.

8. DaVeiga & Eloff (2010):A framework and assessment instrument for information security culture.

The aim of this research for information security should focus on employee behavior, as the organization's success or failure effectively depends on the things that its employees do or fail to do. An information security-aware culture will minimize risks to information assets and specifically reduce the risk of employee misbehavior and harmful interaction with information assets.

Organizations require guidance in establishing an information security-aware or implementing an acceptable information security culture. They need to measure and report on the state of information security culture in the organization.

Various approaches exist to address the threats that employee behavior could pose. However, these approaches do not focus specifically on the interaction between the behavior of an employee and the culture in an organization. Organizations therefore have need of a comprehensive framework to cultivate a security-aware culture.

The objective of this paper is to propose a framework to cultivate an information security culture within an organization and to illustrate how to use it.

An empirical research is performed to aid in validating the proposed Information Security Culture Framework.

9. **Albrechtsen & Hovden (2010):Improving information security awareness and behavior through dialogue, participation and collective reflection. An intervention research.**

The paper discusses and evaluates the effects of an information security awareness program. The program emphasized employee participation, dialogue and collective reflection in groups.

The intervention consisted of small-sized workshops aimed at improving information security awareness and behavior. An experimental research design consisting of one survey before and two after the intervention was used to evaluate whether the intended changes occurred.

Statistical analyses revealed that the intervention was powerful enough to significantly change a broad range of awareness and behavior indicators among the intervention participants. In the control group, awareness and behavior remained by and large unchanged during the period of the research. Unlike the approach taken by the intervention studied in this paper, mainstream information security awareness measures are typically top-down, and seek to bring about changes at the individual level by means of an expert-based approach directed at a large population, e.g. through formal presentations, e-mail messages, leaflets and posters.

This research demonstrates that local employee participation, collective reflection and group processes produce changes in short-term information security awareness and behavior.

10. Van Niekerk& Von Solms(2010):Information security culture: A management perspective.

The aim of the research for Information technology has become an integral part of modern life. Today, the use of information permeates every aspect of both business and private lives. Most organizations need information systems to survive and prosper and thus need to be serious about protecting their information assets. Many of the processes needed to protect these information assets are, to a large extent, dependent on human cooperated behavior. 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.

This paper briefly examines the generic concept of corporate culture and then borrows from the management and economical sciences to present a conceptual model of information security culture.

The presented model incorporates the concept of *elasticity* from the economical sciences in order to show how various variables in an information security culture influence each other.

The purpose of the presented model is to facilitate conceptual thinking and argumentation about information security culture.

11. Hung, et..al, (2010):Perception of information security.

The objective of this research was to investigate people's perception of information security and to unveil the factors that influence people's perception of different threats to information security.

In the survey research, 602 respondents were asked to evaluate one of 21 common threats to information security with regard to its rank related to each of the 20 threat-related features. An exploratory factor analysis was then conducted, and a six-factor structure was derived, which includes factors of Knowledge, Impact, Severity, Controllability, Possibility and Awareness. Using this factor structure, the characteristics of the five most dangerous threats (hackers, worms, viruses, Trojan horses and backdoor programs) and the five least dangerous threats (spam, piratical software, operation accidents, users' online behavior being recorded and deviation in quality of service) were discussed and compared.

The relationships between the factors and the perceived overall danger of threats were found and then tested by multiple regression analyses. Significant effects were also found in people's perception of information security related to computer experience and types of loss.

12. Kraemer, et..al,(2009):Human and organizational factors in computer and information security: Path ways to vulnerabilities.

Aimed to identify and describe how the organizational and human factors related to technical issues and information security.

The research sample consisted of 5 totals for each group includes 8 people working in the technological field in the United States of America.

The research found many of the results, most notably the presence of the correlation between the organizational and human factors technical issues and information security.

13. **Kolb & Abdullah (2009):Developing an Information Security Awareness Program for a Non-Profit Organization.**

This article illustrates the developing information security awareness program for non-profit organizations.

The research was based on achieving its objectives on the previous review of the literature related to information security.

The research found many of the results, most notably that the implementation of information security awareness program is an essential component of the infrastructure of information security, and that there are many risks facing the information security organizations face regular equally faced by non-profit.

14. **Shaw, et..al, (2009):The impact of information richness on information security awareness training effectiveness.**

This research provides a report on the impact of multimedia to increase awareness of information security through the three levels of awareness and embodied cognition, understanding, and protection.

To achieve the objectives of the research, the researchers adopted a theoretical literature review on the security of information and awareness of information security.

The research found many of the results, notably: that learners who have a high level of awareness and understanding enables them to improve the level of protection, and that the learners through written materials have a high level of protection and, finally, that learners from multiple sources reside more level of understanding and perception.

15. **Siponen & Willison (2009):Information security management standards: Problems and solutions.**

The aim of the researchat the problems and solutions developed for information security management standards, in addition to providing a guide improves public requirements and mechanisms for information security.

To achieve this research sought to review the theoretical literature related to information security and former researchers reached this matter.

The research found many of the results, most notably the instructions on the management of information security supposed to be seen as a laboratory of materials for the participants in the management of information security.

16. **Knapp, et..al, (2009):Information security policy: an organizational-level process model.**

To protect information systems from increasing levels of cyber threats, organizations are compelled to institute security programs. Because information security policies are a necessary foundation of organizational security programs, there exists a need for scholarly contributions in this important area. Using a methodology involving qualitative techniques, we develop an information security policy process model based on responses from a sample of certified information security professionals. As the primary contribution of this research research, the proposed model illustrates a general yet comprehensive policy process in a distinctive form not found in existing professional standards or academic publications. This research's model goes beyond the models illustrated in the literature by depicting a larger organizational context that includes key external and internal influences that can materially impact organizational

processes. The model that evolved from the data in this research reflects the recommended practices of our sample of certified professionals, thus providing a practical representation of an information security policy process for modern organizations. Before offering our concluding comments, we compare the results of the research with the literature in both theory and practice and also discuss limitations of the research. To the benefit of the practitioner and research communities alike, the model in this research offers a step forward, as well as an opportunity for making further advancements in the increasingly critical area of information security policy.

17. **Humphreys,(2008):Information security management standards: Compliance, governance and risk management.**

This research Aimed to develop a set of standards for information security management through complaints, governance and risk management.

The research to develop a set of standards for information security management, including: privacy, authentication, confidentiality or reliability, integrity, safety, content, and availability of information or service.

18. **Kritzinger& Smith (2008):Information security management: information security retrieval and awareness model for industry.**

The objective of this research to provide the perspective of concepts for model security awareness and retrieve information that can be used by industrial organizations to enhance the level of information security awareness among employees.

The form includes security awareness and retrieve information on the three dimensions, the first associated measurement and control.

The research found that the model focuses on information security in non-technical terms.

19. Ashenden, (2008):Information Security management: A human challenger?

This paper considers to what extent the management of Information Security is a human challenge. It suggests that the human challenge lies in accepting that individuals in the organization have not only an identity conferred by their role but also a personal and social identity that they bring with them to work. The challenge that faces organizations is to manage this while trying to achieve the optimum configuration of resources in order to meet business objectives.

The paper considers the challenges for Information Security from an organizational perspective and develops an argument that builds on research from the fields of management and organizational behavior.

It concludes that the human challenge of Information Security management has largely been neglected and suggests that to address the issue we need to look at the skills needed to change organizational culture, the identity of the Information Security Manager and effective communication between Information Security Managers, end users and Senior Managers.

20. Richard Y. K. Fung, (2008) Knowledge-Centric Information Security

This paper illustrates that User's knowledge of information security is one of the important factor in information security management as 70-80% security incidents occurred due to negligence or unawareness of users.

In this paper they have analyzed the utility of knowledge management tools to rapidly capture, store, share and disseminate the information security related knowledge with the view that it should be effectively applied by the information system users.

They found that the knowledge management tool can be used to enhance the information security.

21. Houria Al-Sharif, (2006): Threats that affect computerized accounting information systems:Case study of the banks in Gaza Strip - Palestine

The objective of this research is to investigate the threats that effect electronic accounting information systems in the working banks in the Gaza strip, to investigate the most important reasons that lead to the occurring of these threats, and to investigate the procedures that prevent the occurring of these threats. The researchers use a special questionnaire that was designed and distributed to serve the research objectives. The collected data was analyzed using SPSS program. The following findings were reached: (1) the threats that affect the accounting information system: do exist , though it happened at low frequency at the working banks in the Gaza strip; (2) the main reason for these threats is the lack of technological ability and qualifications of the

banks employees (3) there is a low number of information technology employees in the banks in the Gaza strip, and the branches depend only on one employee whose job is to keep the operation of information systems, while specialized employees work in the main branch, an these branches are usually found in the West bank. Depending on these findings, the following recommendations are presented (1) secure procedures that assure the work continuity and availability of information systems in crisis cases through using immune equipments that can be able to find present the threats before

their occurrence. (2) perfect controlling security tools for information using all types including paper form, wire or wireless communications and Internet, and working on required laws for information systems security and information networks security. (3) increase the banks employees ability in IT and information security field .

Ninth: Discussion of previous studies.

The followings can be concluded from the previously mentioned studies and the others discussed studies through this thesis:

1. Previous studies dealt with American , European and Arab organizations, but this work create a new thought in our universities.
2. The current research has been applied at the IUG.
3. Previous studies aimed to measure the impact and the relationship and develop a set of standards for information security and communications, but my work realize some different related facts.
4. The current research was primarily aimed to manage the security of information and communication technology in light of the networks technology without archiving our Arabic establishment and its information system.
5. The studies that took places in Arab countries ignored the security management of information and communication technology in light of the networks.
6. This research showed the most important factors that threaten the security of the information and communication system and thus try to solve the system protection problems.

CHAPTER 2

LITERATURE REVIEW

Section1:Introduction.

Section 2:Information Security.

Section 3:Communication Management

Section 4:Networks Technology

Section 5:Information Security and Communication at IUG

Section 1:Introduction

The university is committed to the appropriate use of Information and Communication Technology (ICT) and Services in support of its teaching, research, administrative and service functions. The University acknowledges an obligation to ensure appropriate security for all Information and Communication Technology data, equipments, and processes in its domain of ownership and control. Every member of the University shares this obligation, to varying degrees. The university recognizes that successful implementation of ICT security relies on having well informed Users combined with effective management procedures.(Barney Glover,2011)

The university routinely gathers, stores, maintains, processes, transmits and disposes of records containing information. That information plays a vital role in supporting the University's business processes and customer services, in contributing to operational and strategic business decisions, and in conforming to legal and statutory requirements. Accordingly, information must be protected to a level commensurate with its value to the organization, while still being made available to those who need it (Takemura , 2010).

ICT stimulates the learners to acquire quality research through team work and time management. Education technology visualizes three strategies for the teaching and learning process. They are mass communication individualized learning and group learning. No single technology is suitable for all types of situations in teaching The technology which is less expensive, low time-consuming and highly effective in delivering the contents of student must be considered. Integrating the whole technology with the latest technology is considered to be the best way of educating the learners..(Swaminathan and Sekar:2012)

Future education will be technology-led, skill matched and need-based education. New technologies namely satellite communication, Fiber Optic cable and computers have enhanced educational capabilities. (NCIHST,2010).

ICTs provide an unprecedented ability to collect and process environmental information that far exceeds the capacity of any individual, which may span time durations far beyond that of a human lifetime, and may encompass the entire terrestrial system from the depths of the ocean to upper reaches of the atmosphere. ICTs can help breakdown the complexity of the environment for easy understanding of the impact of human activities on the environment. ICTs can be used in a number of ways in the management of the environment as noted in (ITU, 2008).

Section 2:information security.

Security become more critical and challenging in communications and networking systems when many contents, devices and users get connected to the Internet in these days, and this trend will continue in the future. (San Diego, 2013)

First: Definition of information security:

Information security is defined as policies, procedures and technical standards that are used to prevent unintentional access, theft or destruction of records (Sultan,2009).

Information security is the protection of information and systems from unauthorized access, disclosure, modification, destruction or disruption. (Computing Services Information Security Office).

The three objectives of information security are:

1. Confidentiality
2. Integrity
3. Availability (Computing Services Information Security Office).

There are those who believe that the security of information and communication is a set of processes, procedures and tools taken by sectors or organizations to secure and protect their information and systems from unauthorized access, whether they from within or from outside the sector. (Kritzinger and Smith,2008).

How to protect organizations' information:

The organizations protect and secure their information through:

a. Adoption of security operations to identify the risks.
b. Configure risk management strategies.
c. Application of the strategies.
d. Test those applications.
e. Monitor the work environment to control the risks.(Humphreys,2008).

The contribution of advanced ICTs is often compromised, because of the unacceptably high levels of security breaches experienced (Doherty a et al., 2011).

According to the 2008 Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) Computer Crime and Security Survey, 47% of the 522 respondent firms experienced computer security incidents, such as virus, insider attacks, laptop thefts, denial of service attacks, unauthorized access of data or networks, and bots. The survey also showed that incidents have occurred frequently over the past 12 months, with 47% of

the respondents experiencing 15 incidents, 14%experiencing 610 incidents, and 13% experiencing over 10incidents. The average financial loss per respondent was USD288,618. Information security is a major concern of today's firms(Richardson, 2009).

Second: Stages of the evolution of information security

According to researcher studies to this stage he determined zidane, (2010) tasks which mentioned that stages of development defined by the information security as follows:

1. During the sixties of the last century was the concept of security is about limiting access or access to data by preventing strangers external manipulation of the devices, and was the first appearance of the term computer security, which means protecting computers and databases, and as a result of expansion in the use of computers changed interest to represent control and protection of data. And accompanied by the use of words Data Security and witnessed the seventies transition to the concept of data security to control access to the data, in addition to measures to protect sites computers from disasters, and adopt plans retrieved Fast data, and store extra copies to her and software away from the site computer.
2. In stage eighties and beyond has increased the importance of using the data, and contributed to developments in the field of information and communication technology to allow more than one user to participate in the database, where a focus on microprocessors to move the security of the data to the information in terms of the preservation of information and integration, availability and degree documented to reduce penetration.

Third: Information security objectives

According to Debi Ashenden,(2008) , the goal of information security must be consistent with the objectives of the organization, that to be necessary to achieve a set of requirements, which are:

1. **Confidentiality:** the privacy of customer information or the organization so that you are away from unauthorized access them to see it. Examples used for privacy encryption system, which is of important examples that provide a high level of security for information while maintaining the flexibility in the handling of such data.
2. **Safety:** and that includes making sure not display information and regulations for any kind of change is unauthorized, in other words, the data cannot be happening to her creation, change, or delete from the non-permit, and also means that the data stored in a parts database tables compatible with the corresponding data stored in another part of the databases. For example: you can miss the safety of the data in the database when a sudden interruption of electricity that feeds your server, or when you do not close the database correctly, and also because of deletion of information by mistake by a staff, may get bugs also due to a virus.
3. **Availability:** Availability of information and computer systems and security operations so that they work properly when you need it, and after the application of information security operations.

To achieve the above-mentioned three requirements, confirmed (Shaw, et .. al, 2009) that organizations need to use a set of standards, and these measures fall under three main things:

a. Access Control.
b. Authentication.
c. Auditing.

The symbol of the previous three things abbreviated AAA is the main thing to understand network security and the security of access to the data, and use these three things on a daily basis in the protection of private data and protect your systems from destruction and unintentional. These concepts former supports the concept of security, which includes the privacy, safety and availability of information already mentioned. And the content of the AAA, are: (Siponen & Willison,2009)

a. **Access Control**: The managed control components software or hardware components in terms of prevention or allow access to network resources and can be as represented smart cards or devices footprint or can be hardware networking such as routers or access points for wireless devices to allocate powers to personal files to computer users.
b. **Authentication:** the verification process of the powers of the users on the network resources and user is determined through the use of his name and password or smart cards are then given powers on the basis of identity. These powers are defined by the network administrator.
c. **Auditing:** It is a sure and tracking of powers by monitoring and network resources and is considered one of the most important things in the field of network security, where

hackers are identified and knowledge of methods and tools that have been used to gain access to the network.

Fourth: Elements of information security

The information security strategy is a set of rules relating to access to information, disposition and transfer within the structure depends information is an essential element in improving its performance and achieve its objectives. (Melad ,2006)

The development of strategies and to find ways for the security of information and communication, and legislative measures in this regard, is to ensure the availability of the following items to any information intended to provide adequate protection to them, namely: (diphtheria, 2008)

1. **Privacy:** and related to ensuring security and protection of data and information relating to individuals and companies from illegal access to it.
2. **Ratification**: which includes making sure that those who are using the data entry are the ones who appear on the network; ensure congruence between individuals who appear on the network and between individuals who are trying not to appear when they commit some mistakes.
3. **Protection**: Ensure that the data and information resources cannot be exposed to the illicit use by exposure to the violation by viruses or attacks by others outside the organization.
4. **Confidentiality**: means to make sure that the information is not disclosed nor seen it by persons not authorized to do so.

5. **Authentication:** This means making sure of the identity of the person who is trying to use the information and see if the user is correct that information or not, this is done through the use of passwords for each user.
6. **Integrity**: which refers to making sure that the content of the information is true and is not modified or destroyed or tampered with in any stage of processing or exchange, whether dealing internally in the project or externally by unauthorized persons so is often done because illegal intrusions such as viruses where no one can break the Bank database and changes the account balance for that rests with the institution ensuring the safety of content through a suitable means of protection, such as software and hardware anti-breakthroughs or viruses.
7. **Availability:** built to ensure business continuity information system with all its components and the continued ability to interact with information and services for information sites and assure that the users of such information to prevent their use or accessed illegally undertaken by people to stop the service by a huge amount of absurd messages across the network to the institution's own devices.
8. **Non-Repudiation**: It is intended to ensure that the denial of a person who has performed a certain online information for this procedure, and therefore must provide a method or a way to prove any act done by any person for the person who has done at a certain time, for example, to make sure the arrival of merchandise was purchased via the Internet to its owner, and to prove transfer funds electronically is to use multiple messages such as e-signature and e-authentication.

Sixth: Causes of risks:

The information systems may be exposed to many of the risks that may threaten its security and that due to a combination of factors which are as follows: (sultan,2009).

1. Electronic information systems include a tremendous amount of data and therefore it is difficult to work hard copies.
2. Difficult to detect errors resulting from a change in the information system, because it cannot handle or read their records only by the computer, which does not reveal any change.
3. Difficulty review of actions that take place through the computer because it is visible and invisible.
4. The difficulty of changing automated systems compared to manual systems.
5. The possibility of their automated systems to misuse by experts not affiliated with the organization in the event they are called to develop systems.
6. May lead risks to automated systems to destroy all records of the organization, and this is far more serious on automated systems from manual systems.
7. Drop documents from which to review the system lead to lower security status hand.

8. The possibility of their automated systems to errors or misuse of the system in the operational phase of the data and the multiplicity of operations in an automated system.
9. Weak control over the automated system due to direct contact with the user information systems.
10. Technological development in remote communication easy communication, process information systems from anywhere and thus the possibility of unauthorized access or misuse of information systems.
11. Use many applications in different locations for the same database leads to the possibility of impenetrable computer viruses and thus the ability to destroy or change the database information system.

Seventh: Types of risks:

There are many risks that could be facing information systems, as mentioned by Baskerville & Siponen ,(2009).

Penetrate systems: This is achieved by entering a person not authorized to do so to the computer system and unauthorized activities as modification application software and steal confidential data or destroy files or software or system or just for illicit use. This is achieved intrusion traditionally through the activities of (masking and disguise) and is intended to demonstrate the person breached that another person authorized to enter or by exploiting weaknesses in the system exceed control measures and

protection, or through information gathered by the person breached sources material or moral, As exploration in garbage facility for passwords or information about the system or through social engineering as an entree person to sensitive information sites within the system as key words or phone calls.

1. **Assault on a field Authorization:** This is done by having the person authorized to use the system for the purpose of what to use in other than this purpose without gets authorization so, and this risk is one of the dangers of Interior in the field of system abuse by the staff of the organization, it may be also external threats, such as the use of penetrating account of a person authorized to use the system by guessing the password or exploiting a system vulnerability to enter the path of a project or part of a project and then doing illegal activities.
2. **Agriculture Weaknesses:** This usually results in danger to storm by someone other than an authorized or through user project exceeded the limits of the authorization granted to it so that the person planting the entrance to what would bring him break later. Among the most famous examples of growing risks Trojans, which is a program lead a legitimate purpose in the apparent but can be used in secret to do actively illegal, was used word processing program ostensibly to edit and format text while having as its purpose the real print all system files and transfer them to a hidden file so penetrative can print this file and get the contents of the system.

3. **The monitor of Communications**: It will be able offender without penetrating a victim's computer to obtain confidential information is often information that facilitates a future breakthrough system simply by monitoring communications from one of the focal points or rings.
4. **Interception of communications:** that is intercept data transmitted during the transfer process without penetrating the system and being the amendments that are commensurate with the purpose of assault and includes symptoms communications to create Intermediate System place, so that the user to pass through and provides system sensitive information on a voluntary basis.
5. **Denial / DoS Denial of service attack**: This is done through activities prevent user speed of access to information or access the service and the most prominent patterns denial of service Send large amount of e-mail messages at once to a specific location in order to overthrow the regime future inability to endure or directing a large number of Internet addresses in a way that does not allow the segmentation process materials sent packages leads to overcrowding server and its inability to deal with it.
6. **Not recognizing by doing the act**: The danger in not adopting the person of the addressee, or sender act passed him, as if denying that it is not the person who sent the request purchase online. And launched strategic actors from the ability to summarize system continuous risk analysis process and identify the needs of protection, and risk analysis process is in fact an integrated system of analysis and safety act starts from good preparation based on

understanding and knowledge and identify the elements of the system, processes and risks, and then specify the criteria for the threat and the scope of protection required to and depending on his means of protection, ending a statement accepted standard loss to imagine achieved regardless of the level of protection and the level of preparedness for a confrontation.

Eighth : Threats facing information security:

The start of a new year is a great time for companies to evaluate their information security practices and begin thinking about what threats they'll be facing in the coming year," said Kevin Prince, CTO, Perimeter E-Security. As these security threats are becoming more serious and difficult to detect, it is vital for companies to understand what they can do to best protect their systems and information.

1. **Top 10 information security threats for 2010 :**according to Perimeter E-Security . (http://www.net-security.org)

   Malware

   Last year, Malware was listed as the second highest ranked threat to organizations on Perimeter E-Security's list of top threats. There are many methods to install malware on systems, including the use of client-side software vulnerabilities. Browsers remain a top target for vulnerabilities. In 2009, the FBI reported that for the first time ever, revenue from cybercrime

had exceeded drug trafficking, estimated at taking in more than one billion annually in profits. . (http://www.net-security.org)

a. **Malicious insiders**

Malicious insiders were listed as the top threat for 2009, but have fallen to the #2 spot for 2010. With the downturn in the economy last year, it was no surprise that many desperate and disgruntled employees attempted to exploit the companies they currently or previously worked for. There is no way to eliminate the threat of malicious insiders completely, but through good security policies and followed procedures, the incidents could be a fraction of what they are today. With the economy still suffering and still high unemployment levels, Malicious Insiders will continue to be a threat. . (http://www.net-security.org)

b. **Exploited vulnerabilities**

Vulnerability exploit is at the heart of hacking and data breaches. Worms, viruses, malware, and a host of other attack types often rely on vulnerability exploit to infect, spread and perform the actions cyber criminals want. And yet, organizations are still not doing what they need to for patch management. Hackers are more often exploiting client side vulnerabilities and other vulnerabilities associated with 3rd party applications. . (http://www.net-security.org)

c. **Careless employees**

Careless and untrained insiders will continue to be a very serious threat to organizations in 2010. Insiders can be broken down into three categories: careless & untrained employees, employees that are duped or fall prey to social engineering type attacks, and malicious employees. Protecting a network and critical and sensitive data is done very differently for each type. Policies, procedures, training and a little technology can make a world of difference in reducing an organization's risk to careless insiders. . (http://www.net-security.org)

d. Mobile devices

Mobile devices have become a plague for information security professionals. There are worms and other malware that specifically target these devices such as the iPhone worm that would steal banking data and enlist these devices in a botnet. Theft is still a major cause of data breaches as mobile devices, especially laptops, are the main culprits. Tens of thousands of laptops are stolen each year and often these have sensitive data that require public disclosure as a data breach. . (http://www.net-security.org)

e. Social networking

Social networking sites such as Face book, MySpace, Twitter and others have changed the way people communicate with each other, but these sites can pose serious threats to organizations. One main problem is that there is a trust component to these sites which makes them fertile ground

for identity thieves. There is also a personal safety issue. Social networking sites are a stalker's dream come true. Social networking sites are breeding grounds for SPAM, scams, shareware and a host of other attacks and these threats will continue to rise. . (http://www.net-security.org)

f. Social engineering

Social engineering is always a popular tool used by cyber criminals and phishing is still a popular method for doing just that. In fact, these new venues make social engineering even more effective. This year will have an added measure of complexity when it comes to social engineering attacks. Beginning sometime mid-2010, domain names will be expanded to include Japanese, Arabic, Hindi and even Greek characters, and with all of these characters being available for domain names, no longer will looking at a domain help one determine if it's legitimate or not. . (http://www.net-security.org)

g. Zero-day exploits

Zero-day exploits are when an attacker can compromise a system based on a known vulnerability but no patch or fix exists, and they have become a very serious threat to information security. Zero-day vulnerabilities are being discovered in traditionally very secure protocols such as SSL and TLS. The zero-day vulnerability could also be in providers. . (http://www.net-security.org)

h. Cloud computing security threats

Using cloud based (i.e. Internet based) applications may not be as secure as once thought with many stories in 2009 regarding cloud based security issues. Many are calling for forced encryption to access "in the cloud" services. As cloud computing grows in popularity over the next few years, cloud security will become a very big issue. . (http://www.net-security.org)

i. Cyber espionage

Cyber espionage is a threat that's being heard more and more all the time and there have been a flood of stories in 2009 on this subject. Most of these incidents surround government bodies and agencies and therefore have not been a huge threat to most individual organizations. However, since cyber espionage has major implications for the government, it is a rising threat that must be closely monitored.(Kevin Prince, CTO, Perimeter E-Security:2010)the issue of security of information systems of important issues and necessary should the company be taken into account and develop a plan comprehensive protection within their means organizational and material must be such protection is strong and not weak. (http://www.net-security.org)

2. **Requirements to protect the security of information systems are:**

    a. A general protection policy for the security of information systems is determined by the nature of the work and organization applications.

    b. Should senior management in the organization support the security of their information systems.

    c. Should be entrusted with the responsibility of the security of information systems in the organization for specific individuals.

    d. Determine the necessary protection for the operating systems and applications.

    e. Identify mechanisms for monitoring and inspection of information systems and computer networks.

    f. Keep backup copies of secure information systems.

    g. Encrypt information that is saved and stored and transported to various media.

    h. Secure the continuity of the work and the readiness of information systems, especially in a crisis situation and face the risks related to information systems..(tara& Zbibi, 2006)

Ninth: Tools of information security:

The most important means of information security are:

1. **Early detection of breakthroughs:** This is done by the system registry file, and commands, and the operating system, and Task Manager, which displays all the programs and the program is recognized.
2. **Network Protection**: protect the network internally to take a series of actions, including the training of personnel in the network to deal with the security measures taken in the organization that contains the network.
3. **Encryption arbitrator**: to ensure that no unauthorized access to the system and the work schedule for re-encryption so it does not get its symbols to others, and the protection of electrical wiring and network extensions until one cannot break through it.
4. **Firewall:** The wall fiery software and hardware working on the nomination of data entering the database before it reaches the server and thus the firewall book up from the external network does not want to play in the internal network, and comes a firewall in the form of a wave brow Screening Router or in the form of more the effectiveness of such intermediary proxy so that he can understand the protocol used and interpreted.
5. **Antivirus:** a collection of programs that address the virus entering the device, and vary antiviral in terms of power and efficiency, but it can for virus makers and publishers exceeded effect often.

6. **Multiple servers:** It means multiple servers using server for each system or each group systems linked by a functional relationship, such as circulars, Transactions confidential, regulations and laws, investigations, wanted, Administrative Affairs, Public officers and individuals, as the presence of all these systems in a single server increases the likelihood of penetration and distribution of all systems and multiplicity leads to the decline of the problem in a single server and a single system.

Tenth: 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).

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.

2. ISO/IEC 27001 requires that management:

a. Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts.

b. 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.

c. 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.

3. The Key Benefits of 27001 are:

a. 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 .

b. Provides confidence and assurance to trading partners and clients; acts as a marketing tool.

c. Allows an independent review and assurance to you on information security practices .

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

a. It is suitable for protecting critical and sensitive information

b. It provides a holistic, risked-based approach to secure information and compliance

c. Demonstrates credibility, trust, satisfaction and confidence with stakeholders, partners, citizens and customers

d. Demonstrates security status according to internationally accepted criteria

e. Creates a market differentiation due to prestige, image and external goodwill

f. If an organization is certified once, it is accepted globally.

5. 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:

a. Security policy
b. Organization of information security
c. Asset management
d. Human resources security
e. Physical and environmental security
f. Communications and operations management
g. Access control
h. Information systems acquisition, development and maintenance
i. Information security incident management
j. Business continuity management
k. 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).

Eleventh :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.

1. **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.
2. **Do (implementing and workings of the ISMS):** Implement and exploit the ISMS policy, controls, processes and procedures**.**

3. **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.
4. **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

Twelve :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.

Thirteenth :Control objectives and controls

1. Security Policy

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

Organization of information security

b. Internal organization: To manage information security within the organization.

c. 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.

2. Asset Management

a. Responsibility for assets: To achieve and maintain appropriate protection of organizational assets.

b. Information classification: To ensure that information receives an appropriate level of protection.

3. Human resources security

a. 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.

b. 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.

c. Termination or change of employment: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

4. Physical and environmental security

a. Secure areas: To prevent unauthorized physical access, damage and interference to the organization‘s premises and information.

b. Equipment security: To prevent loss, damage, theft or compromise of assets and interruption to the organization‘s activities.

5. Communications and operations management

a. Operational procedures and responsibilities: To ensure the correct and secure operation of information processing facilities.

b. 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.

c. System planning and acceptance: To minimize the risk of systems failures.

d. Protection against malicious and mobile code: To protect the integrity of software and information.

e. Back-up: To maintain the integrity and availability of information and information processing facilities.

f. Network security management: To ensure the protection of information in networks and the protection of the supporting infrastructure.

g. Media handling: To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.

h. Exchange of information: To maintain the security of information and software exchanged within an organization and with any external entity.

i. Electronic commerce services: To ensure the security of electronic commerce services, and their secure use.

j. Monitoring: To detect unauthorized information processing activities.

6. Access control

a. 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.

b. User responsibilities: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.

c. Network access control: To prevent unauthorized access to networked services.

d. Operating system access control: To prevent unauthorized access to operating systems.

e. Application and information access control: To prevent unauthorized access to information held in application systems.

f. Mobile computing and teleworking: To ensure information security when using mobile computing and teleworking facilities.

7. Information systems acquisition, development and maintenance

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

b. Correct processing in applications: To prevent errors, loss, unauthorized modification or misuse of information in applications.

c. Cryptographic controls: To protect the confidentiality, authenticity or integrity of information by cryptographic means.

d. Security of system files: To ensure the security of system files.

e. Security in development and support processes: To maintain the security of application system software and information.

f. Technical Vulnerability Management: To reduce risks resulting from exploitation of published technical vulnerabilities.

8. Information security incident management

a. 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.

b. Management of information security incidents and improvements: To ensure a consistent and effective approach is applied to the management of information security incidents.

9. Business continuity management

a. 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.

10. Compliance

a. Compliance with legal requirements: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

b. Compliance with security policies and standards, and technical compliance: To ensure compliance of systems with organizational security policies and standards.

c. Information systems audit considerations: To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

Section3:Communication Management

First: Introduction

The concept of communication is recognized as an essential component in personal relationships. Without communication, an information breakdown can take place resulting in relational difficulties' and in extreme circumstances, may even result in illness. Although there are various methods of communication available that seem sufficient for sharing information, e.g. face-to-face meetings, phone calls, letter writing, and e-mails, communication methods and devices continue to been enhanced and developed.

1. The definition for communication

A message sent between people, remains the same; but the method of transmitting the message changes. The degree of importance that a person places on the information to be shared with respect to time, subject matter, and the kind of relationship existing between the communicating parties helps to determine the method of transaction. Not only have the communication utilities available in mobile phones improved, but the innovation of the Smartphone has increased the methods for exchanging information. A Smartphone is a mobile phone with built-in applications, i.e. video player, MP3 player, television, camera, with the ability to access the Internet (PCMAG.com, 2009).

In recent decades international management itself as a separate component of the general science of leadership, is an intercultural management. In this context of globalization, computerization, any business that wants have a modern management should have a structured information system based on communication, overall objective consisting in

providing accurate data in real time all parties, increasing the level of communication. Given these considerations, we conducted this work trying to highlight the role of communication in achieving a modern, emphasizing international management features. The paper is divided into 6 parts, prefaced by an introduction of the paper we presented and completed within a set of conclusions on the effectiveness of communication. During the other paragraphs, we present the theoretical concepts of international management, communication, after which I stressed the role of information communication, managerial communication and will then focus on the process, taking stock of its specific stages in international management.(Vasile G, (2012)

The utilization of the Smartphone is changing the social availability of people through the use of its various applications and utilities. Relationships that exist professionally and personally are susceptible to structural shifts as smart phones effect personal privacy while blending and expanding social networks (Lugano, 2008).

It is the process of transfer of information from the sender to receiver. Today communication skills are equally important acknowledge and technological skills. There are four components in the process of communication. There are the basic elements of ICT are communication, storage and retrieval of knowledge. Libraries, besides the repositories of books and journals, now become access points for data bases, websites and a range IT based products. ICT stimulates the learners to acquire quality research through team work and time management. Education technology visualizes three strategies for the teaching and learning process. They are mass communication, individualized learning and group learning.

The technology which is less expensive, low time-consuming and highly effective in delivering the contents of students 'information and knowledge must be considered. Integrating the whole technology with the latest technology is considered to be the best way of educating the learners Bates has outlined the developments in ICT with implications for learning. They are:

a. Integration of TV, Telecommunication and computers through digitization and compression techniques.
b. Reduced costs and flexible user applications of Telecommunications, through developments such as ISDN / Fiber optics / Cellular radios Services. (Swaminathan and Sekar:2012).

Communications technologies are evolving fast, following the demand for more and newer services anywhere and at anytime. The drivers for this trend come from the economy, military defense, health and education fields, and match the request for more efficiency, and more comfortable and safe daily life. As a rule, new technologies are put into use as soon as they are available.

The many technological developments accomplished in the last decades have a direct impact on communication networks. Nevertheless, all hardware and software technological improvements or implementations can be the source of new vulnerabilities for the systems and services that rely upon them. The statistical reports about the changing intensity and type variety of security vulnerabilities and attacks show that integrity, reliability and availability problems are far from being solved .(IBM Internet Security Systems (X-Force, 2009).

Section4:Networks Technology

First: the definition Networks Technology

the definition of group/network is in general open ended and is subject to researcher discretion. Broadly, reference group for a person is defined by the individuals whose mean outcome and characteristics influence the individual's own. Here, we argue that reference groups defined solely based on geographical proximity do not fit the Indian context given the social fragmentation that is at the forefront of the social structure, especially in the rural areas. The reference group of a farmer in a particular village could comprise farmers in a village other than his own who belong to the same caste group. Our construction of reference groups is along the lines of (Fontaigne and Yamada :2011).

Last years have known the development of small, low cost, low power and multifunctional sensor nodes, having the possibility of sensing and collecting application specific data as temperature, pressure and movement to allow environment monitoring. (John Wiley & Sons, Hobo- ken, 2009.)

Second: Computer networks

When two or more computers are interconnected to each other via some kind of medium to share resources then the state is called computer network.

Computer network is the interconnection of computers for communication purposes.

Third: Connection method

Computer networks can also be classified according to the hardware and software technology that is used to interconnect the individual devices in the network, such as Optical fiber, Ethernet, Wireless LAN, Home PNA, Power line communication or G.hn. Ethernet uses physical wiring to connect devices. Frequently deployed devices include hubs ,network switches, network bridges and/or routers.

Wireless LAN technology is designed to connect devices without wiring. These devices use radio waves or infrared signals as a transmission medium.

Ethernet over coax technology uses existing home wiring (coaxial cable, phone lines and power lines) to create a high-speed (up to 1 Gigabit/s) local area network.

Fourth: Wired technologies

Twisted pair - This is the most widely used medium for telecommunication. Twisted-pair wires are ordinary telephone wires which consist of two insulated copper wires twisted into pairs and are used for both voice and data transmission. The use of two wires twisted together helps to reduce crosstalk and electromagnetic induction. The transmission speed range from 2 million bits per second to 100 million bits per second.

Coaxial cable – These cables are widely used for cable television systems, office buildings, and other worksites for local area networks. The cables consist of copper or aluminum wire wrapped with insulating layer typically of a flexible material with a high dielectric constant, all of which are surrounded by a conductive layer. The layers of insulation help minimize interference and distortion. Transmission speed range from 200 million to more than 500 million bits per second.

Fiber optics – These cables consist of one or more thin filaments of glass fiber wrapped in a protective layer. It transmits light which can travel over long distance and higher bandwidths. Fiber-optic cables are not affected by electromagnetic radiation. Transmission speed could go up to as high as trillions of bits per second. The speed of fiber optics is hundreds of times faster than coaxial cables and thousands of times faster than twisted-pair wire.

Fifth: Wireless technologies

Terrestrial microwave – Terrestrial microwaves use Earth-based transmitter and receiver. The equipment look similar to satellite dishes. Terrestrial microwaves use low-gigahertz range, which limits all communications to line-of-sight. Path between relay stations spaced approx. 30 miles apart. Microwave antennas are usually placed on top of buildings, towers, hills, and mountain peaks.

Communications satellites – The satellites use microwave radio as their telecommunications medium which are not deflected by the Earth's atmosphere. The satellites are stationed in space, typically 22,000 miles above the equator. These Earth-orbiting systems are capable of receiving and relaying voice, data, and TV signals.

Cellular and PCS Systems – Use several radio communications technologies. The systems are divided to different geographic area. Each area has low-power transmitter or radio relay antenna device to relay calls from one area to the next area.

Wireless LANs – Wireless local area network use a high-frequency radio technology similar to digital cellular and a low-frequency radio technology. Wireless LANS use spread

spectrum technology to enable communication between multiple devices in a limited area. Example of open-standard wireless radio-wave technology is IEEE 802.11b.

Bluetooth – A short range wireless technology. Operate at approx. 1Mbit/s with range from 10 to 100 meters. Bluetooth is an open wireless protocol for data exchange over short distances.

The wireless Web – The wireless web refers to the use of the World Wide Web through equipment like cellular phones, pagers, PDAs, and other portable communication devices. The wireless web service offers anytime/anywhere connection .

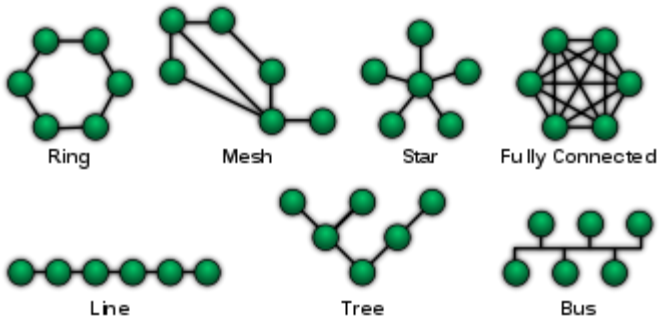
Sixth: Scale

Networks are often classified as LAN, WAN, MAN, PAN, VPN, CAN, SAN, etc. depending on their scale, scope and purpose. Usage, trust levels and access rights often differ between these types of network - for example, LANs tend to be designed for internal use by an organization's internal systems and employees in individual physical locations (such as a building), while WANs may connect physically separate parts of an organization to each other and may include connections to third parties.

Seventh: Functional relationship (network architecture)

Computer networks may be classified according to the functional relationships which exist among the elements of the network, e.g., Active Networking, Client-server and Peer-to-peer (workgroup) architecture.

Figure (2.1) Network topology



Network Topologies examples

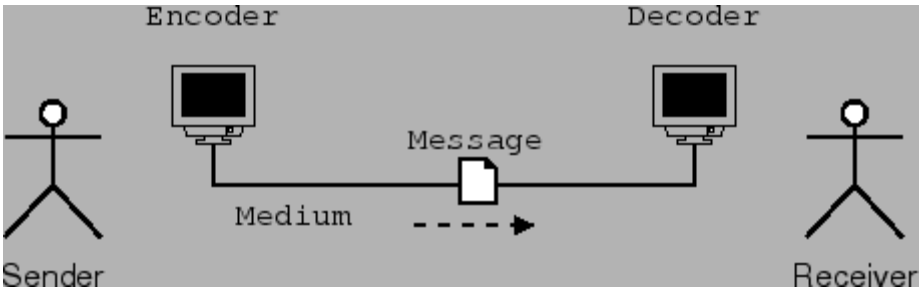
Computer networks may be classified according to the network topology upon which the network is based, such as bus network, star network, ring network, mesh network, star-bus network, tree or hierarchical topology network. Network topology signifies the way in which devices in the network see their logical relations to one another. The use of the term "logical" here is significant. That is, network topology is independent of the "physical" layout of the network. Even if networked computers are physically placed in a linear arrangement, if they are connected via a hub, the network has a Star topology, rather than a bus topology. In this regard the visual and operational characteristics of a network are distinct; the logical network topology is not necessarily the same as the physical layout. Networks may be classified based on the method of data used to convey the data, these include digital and analog networks.

Eighth: OSI-ISO Model

The Open System Interconnection Reference Model (OSI Reference Model or OSI Model) is an abstract description for layered communications and computer network protocol design. It was developed as part of the Open Systems Interconnection (OSI) initiative. In its most basic form, it divides network architecture into seven layers which, from top to bottom, are the Application, Presentation, Session, Transport, Network, Data-Link, and Physical Layers. It is therefore often referred to as the OSI Seven Layer Model.

A layer is a collection of conceptually similar functions that provide services to the layer above it and receives service from the layer below it. On each layer an instance provides services to the instances at the layer above and requests service from the layer below. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of the path. Conceptually two instances at one layer are connected by a horizontal protocol connection on that layer.

Figure (2.2) General communication model



General Communication Model

The parts of this model are as follows:

Sender: The sender is what or who is trying to send a message to the receiver.

Encoder: In the general case, it is not possible to directly insert the message onto the communications medium. For instance, when you speak on the telephone, it is not possible to actually transmit sound (vibrations in matter) across the wire for any distance. In your phone is a microphone, which converts the sound into electrical impulses, which can be transmitted by wires. Those electrical impulses are then manipulated by the electronics in the phone so they match up with what the telephone system expects.

Message: Since this is a communication engineer's model, the message is the actual encoded message that is transmitted by the medium.

Medium: The medium is what the message is transmitted on. The phone system, Internet, and many other electronic systems use wires. Television and radio can use electromagnetic radiation. Even bongo drums can be used as a medium .

Decoder: The decoder takes the encoded message and converts it to a form the receiver understands, since for example a human user of the phone system does not understand electrical impulses directly.

Receiver: The receiver is the target of the message.(Hallberg, Bruce A.:2009)

Section 5: Information Security At Islamic University Of Gaza.

First: About the Islamic University of Gaza

IUG is an independent academic institution located in Gaza. IUG is a home to the well-planned programs, a way to the different community levels and a place for researchers and good teachers. IUG is a member of four associations: International Association of Universities, Community of Mediterranean Universities, Association of Arab Universities and Association of Islamic Universities. Prior to the establishment of the Islamic University, students of Gaza Strip had to seek their higher education in Egypt because Gaza Strip lacked universities by them. In 1967, it deemed necessary to a group of businessmen to establish a higher education institution in Gaza Strip to serve thousands of students and to help them save their time, money and effort. On that account was the establishment of Islamic University in 1978 starting with three faculties only, IUG developed its facilities and academic14departments to have ten faculties at the moment to offer BA. B.Sc., MA, M.Sc., Diploma and higher diploma in a variety of disciplines. There are almost 18,206 students at IUG including 6,723 male students and 11,4843female students (IUG, 2011).

Second: Computer systems department:

this department of the primary partitions in the Department of information technology infrastructure, where it provides services to approximately 3,000 computer and peripherals connected to the University network, as well as various network services (file – online – email – wireless network services-hosting services-and many others ...) to members of the administrative and teaching staff, as well as university students.((IUG, 2013)

The work of this department:

1. support development and implementation of operating systems and software for network infrastructure, and all related services.
2. follow-up to new technological developments for network servers (Servers), to improve the services offered to users.
3. follow-up to modern software, as well as new versions of the software currently in use, with a view to integration into the working environment.

Third: Communication department:

Communications Department is one of the most important departments in the University, and the Department overseeing the technical equipment in the University and related information technology services directly or indirectly. (IUG, 2013).

The work of this department:

1. supervise University function and ensure its development functions.
2. supervise systems of Visual communication.
3. supervision of electronic security systems.
4. support for SMS.
5. maintenance and installation of phonetics at the University.

Fourth: Networks Department:

there are thousands of devices connected to the University Network (computers, printers, cameras ...)And these devices benefit from services provided by the network, this section for connecting equipment management and supervision.

The work of this department:

1. the planning and management of the network infrastructure on university.
2. follow-up to the Internet with the Internet provider.
3. follow-up to the wireless network on campus.
4. monitor network performance through special software.

Fifth: User accounts department:

user accounts section of the primary partitions and provided substantive and technical support services immediately required for each of the user accounts where we have 2500 network account and electronic mail to permanent staff and private contracts, in addition to approximately 22,000 students have accounts on the University network.

The work of this department:

1. providing substantive support and advisory service for staff and students of the users of the systems and networks to ensure optimal operation.

   management of network accounts for University staff (create new accounts – operations relating to existing accounts)
2. accounts databases of administrative staff.
3. manage email accounts for employees and university students as well as staff reserve mail.

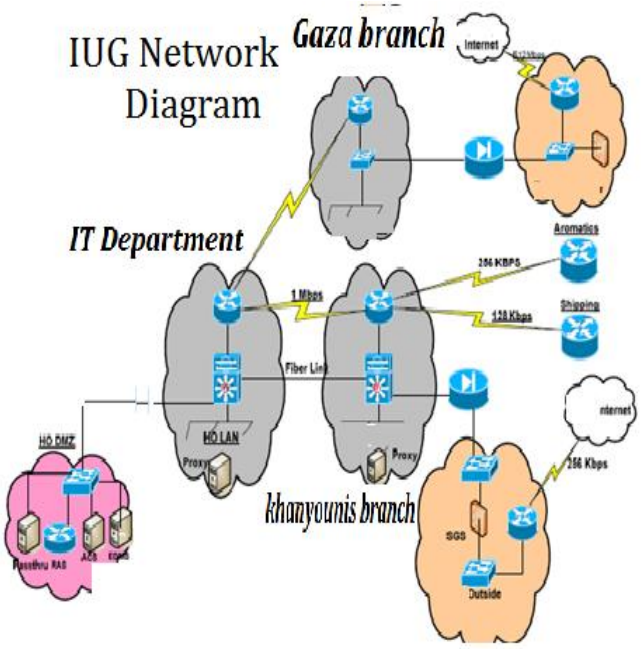
4. management of Internet subscriptions.
5. the file storage service management and related powers to the benefit of the work.
6. work to monitor errors and technical notes and the handle and propose solutions.
7. preparation of advertising guidelines for information systems to increase performance and efficiency, particularly emerging ones.
8. any other functions within its competence.(www.iug.edu.ps)

Sixth: Islamic University consists of two main sites

as shown in Figure (2.3).

1. the main office in the Gaza Strip.
2. Branch Office in the southern Gaza Strip.

Figure (2.3) IUG Networks Diagram



(Designed by researcher)

The University seeks always to the acquisition and application of the latest technologies in the field of information systems and security, which is a key factor to maintain the degree and quality of the performance and security of information systems.

Islamic University networks are designed primarily using nets and protective equipment by CISCO company and the information security system is currently at the Islamic University on the following:

1. strategy and information security policies: It is about the laws and regulations that govern the company's information security.
2. technical information systems and networking environment its organs and systems and software as will be explained in the following pages:

seventh: the information security at the Islamic University

through a network technology consists of several components, including:

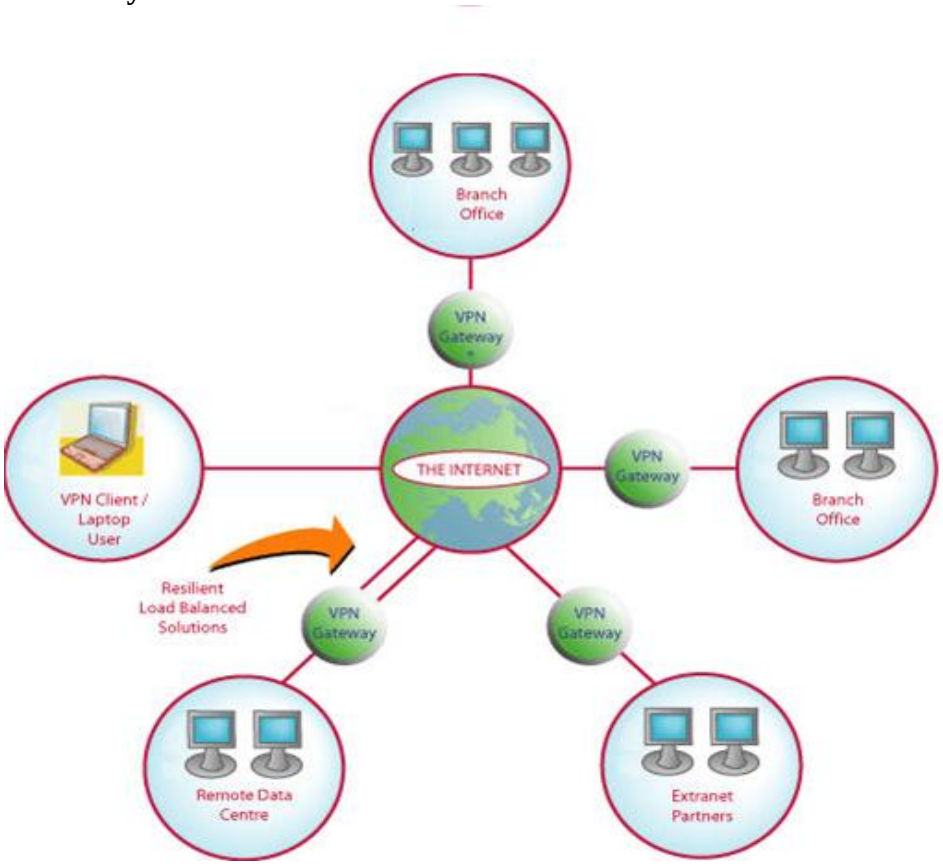
1. **Local Area Network**: a local network scope, be contained within the Office, or a group of offices within a single building, and to provide such great speed networks for the exchange of data and resources which the user feels that these resources stored on his PC. The networks Local Area Network commonly used one type of communication media and sometimes more than one type, and these arguments are one of the following: wire double wrapped Twisted Pair Cable and these wires either covered or not covered with protective Shielded or Unshielded, and coaxial cable Coaxial cable, wire fiber Optical Fiber Optic Cable, and contact center wireless transmission media used the university type I and III of the wire, and effects that in

case of an interruption line fiber main SAA nutritious sections angled service and there is no line reserves to feed sections leading to the stoppage of work. In the case of fiber line break between the main office-related and second branch will cease to operate in the second section briefly until satellite formed. In general when any defect Viper will affect the work of the loss of time and loss of funds.

2. **Wireless networks**: a network based on radio waves to exchange information instead of traditional cables. Can be likened to a computer that is connected to a wireless network mobile phone, the similarity here is the possibility to use the device without network connection cable. Also uses the term Wi-Fi is usually to refer to the wireless network. The places to use Wi-Fi at the university, it is in all the meeting rooms and in the senior management suite will be installed the main office.
3. **Virtual privacy phantom network Virtual Private Network**: It is a channel of communication is documented and coded stretches across a public network, such as the Internet. Because of this network is not available where a safety, data protection during transport encrypted. Based network privacy phantom on a protocol known as the Point-to Point Tunneling Protocol, and network features privacy phantom it works independently of service Contact usual, technology comprises network privacy phantom is an alternative communication telephony, that is, all information exchanged between the two host are transported across this encrypted channel and therefore security checks for non-penetrating information or sabotage. And working to create a connection equivalent to a private connection between two computers or networks online instead of creating a separate touch my phone. And enables remote users, regardless of their location, communication and interpersonal with university

network as if they were in the company's headquarters, and working to secure the network through the addition of encryption services. In addition to increasing productivity by allowing users to access network resources directly, allowing them to work more effectively what would have happened if the work will be via e-mail or phone or travel to the offices of the university (which provides a lot of money).

Figure (2.4) shows the components of the network privacy phantom at the Islamic University.



4. Firewall: It is a safety device works as a security officer on the borders of the Internet. It constantly looks at traffic involved in the communication process and emerging from it. With regard to the Islamic University there are two layers of the wall of the fire believe the local network from a penetration:

a. Symantec: It is a security gate that protects the university network of illegal penetration through programmed laws and attacks such as viruses. Among the benefits and advantages of this wall is suitable to the needs of the university, regardless of the size of operations and its ability to work Clustering, which increases the effectiveness of the protection of the network.
b. Cisco: It features the use of fictitious network privacy and protection from various types of intrusions, filter and monitor Internet browsing.

c. Switches: It is a multiport device determines how to handle the contents of the data set on the basis of the protocol and data company. The multiple types of routers in the company, and offers directed the following services for network LAN, is the possibility of transmission and reception over the network at the same time, the possibility of the existence of many concurrent connections, and support for networks with high speed, featuring much delay low and high rates of data, and the allocation of flow velocity data depending on the port.

d. Spams: as the university relies on a Symantec program in reducing spam and e-mail server, but still very Symantec primitive program issued spam, the university still in the process of evaluating some products, has been the experience of some products such as Barracuda & Xtream.

Chapter 3
Research Methodology

First: Introduction

Second : Data Collection Methodology

Third : Population of research

Fourth: Personal information

Fifth : Questionnaire content

Sixth: Pilot Research

Seventh : Validity of the Research

Eighth : Reliability of the Research

Ninth : Half Split Method

Tenth : Cronbach's Coefficient Alpha

Eleventh : Statistical Manipulation

Twelve : Statistical methods

First: Introduction

This chapter describes the methodology that was used in this research. The adopted methodology to accomplish this research uses the following techniques: the information about the research design, research population, questionnaire design, statistical data analysis, content validity and pilot research.

Second : Data Collection Methodology :

In order to collect the needed data for this research , the study used the secondary resources in collecting data such as books, journals, statistics and web pages , and preliminary resources are not available in secondary resources through distribute questionnaires on research population to get their opinions about the "information security management in light of network technology ". Research methodology depend on the analysis of data on the use of descriptive analysis, which depends on the poll and use the main program (SPSS).

Third : Population of research

Population consist of employees at IUG work as a Director of the Department or head of section or Officer in the Department of Information Technology , the total of employees 92 and this research will use comprehensive survey.

Fourth : Personal information:

1. Qualification :

Table No.(3.1) show that 3.6% of the sample of qualification are " Diploma " , and 58.9% of the sample of qualification are " B.Sc " , and 32.1% of the sample of qualification are "master " , and 5.4% of the sample of qualification are " Ph.D " .

Table No.(3.1)Qualification

Qualification	Frequency	Percentage
Diploma	2	3.6
B.Sc	33	58.9
Master	18	32.1
Ph.D	3	5.4
Total	56	100.00

B.Sc and master categories record the highest frequency and percentage

2. Gender

Table No.(3.2) show that 80.4 % from the samples are " male" , and 19.6% from the samples are " female"

Table No.(3.2)Gender

Gender	Frequency	Percentages
Male	45	80.4
Female	11	19.6
Total	56	100.0

Male gender records the highest values

3. Age

Table No.(3.3) show that 23.2 % of the samples age are " Less than 25 years " , and 50.0% of the samples age are " 25 to 34 years " , and 21.4% of the samples age are "35 to 44 years " , and 5.4% of the samples age are " more than 45 years " .

Table No.(3.3)Age

Age	Frequency	Percentages
Less than 25 years	13	23.2
25 to 34 years	28	50.0
35 to 44 years	12	21.4
more than 45 years	3	5.4
Total	56	100.0

25-34 years category records the highest frequency and percentages

4. Job title

Table No.(3.4) show that 7.1% of the samples job are " Director of the Department " , and 25.0 % of the samples job are " head of section " , and 67.9% of the samples job are " Officer in the Department of Information Technology " .

Table No.(3.4)Job title

Job title	Frequency	Percentages
Director of the Department	4	7.1
head of section	14	25.0
Officer in the Department of Information Technology	38	67.9
Total	56	100.0

5. Number of experience years in the current position

Table No.(3.5) show that 39.3% of the samples of **experience in the Current Position** "5 years and less " , and 41.1% of the samples of **experience in the Current Position** "6 to 10 years " , and 16.1% of the samples of **experience in the Current Position** " 11 to 15 years " , and 3.6 % of the samples of **experience in the Current Position** "16 years and more ".

Table No.(3.5)number of experience years in the Current Position

number of experience years in the Current Position	Frequency	Percentages
5 years and less	22	39.3
6 to 10 years	23	41.1
11 to 15 years	9	16.1
16 years and more	2	3.6
Total	56	100.0

5 years and less ,from 6 to 10 years options recored the highest frequency and percentages

Fifth : Questionnaire content

questionnaire was provided with a covering letter explaining the purpose of the research, the way of responding, the aim of the research and the security of the information in order to encourage a high response. The questionnaire included multiple choice question: which used widely in the questionnaire, The variety in these questions aims first to meet the research objectives, and to collect all the necessary data that can support the discussion, results and recommendations in the research.

The sections in the questionnaires will verify the objectives in this research related to information security management in light of network technologies as follows

First section : personal data consist of 5 Sentences.

second section : related to information security management in light of network technologies and divided into six fields as follows

1. Risks of input data consist of 7 Sentences
2. Risks of output data consist of 8 Sentences
3. Surrounding Technology Risks consist of 6 Sentences
4. The lack of experience and training risks consist of 5 Sentences
5. The weakness of control procedure risks of from 7 Sentences
6. Policies and procedures consist of 15 Sentences

The Instruments of the research consist as follow:

Level	**Strongly disagree**	**Disagree**	**Hesitant**	**Agree**	**Strongly agree**
Scale	1	2	3	4	5

Sixth : Pilot Research

A pilot research for the questionnaire was conducted before collecting the results of the sample. It provides a trial run for the questionnaire, which involves testing the wordings of question, identifying ambiguous questions, testing the techniques that used to collect data, and measuring the effectiveness of standard invitation to respondents , the research used 20 pilot questionnaire .

Seventh : Validity of the Research

We can define the validity of an instrument as a determination of the extent to which the instrument actually reflects the abstract construct being examined. "Validity refers to the degree to which an instrument measures what it is supposed to be measuring". High validity is the absence of systematic errors in the measuring instrument. When an instrument is valid; it truly reflects the concept it is supposed to measure. Achieving good validity required the care in the research design and sample selection . The amended questionnaire was by the supervisor and three expertise in the tendering and bidding environments to evaluate the procedure of questions and the method of analyzing the results. The expertise agreed that the questionnaire was valid and suitable enough to measure the purpose that the questionnaire designed for.

1. Content Validity of the Questionnaire

Content validity test was conducted by consulting two groups of experts. The first was 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. The other was requested to evaluate that the instrument used is valid statistically and that the questionnaire was designed well enough to provide relations and tests between variables. The two groups of experts did agree that the questionnaire was valid and suitable enough to measure the concept of interest with some amendments.

2. Statistical Validity of the Questionnaire

To insure the validity of the questionnaire, two statistical tests should be applied. The first test is Criterion-related validity test (Pearson test) which measure the correlation coefficient between each item in the field and the whole field. The second test is structure validity test (Pearson test) that used to test the validity of the questionnaire structure by testing the validity of each field and the validity of the whole questionnaire. It measures the correlation coefficient between one filed and all the fields of the questionnaire that have the same level of similar scale.

3. Criterion Related Validity :

Internal consistency:

Internal consistency of the questionnaire is measured by a scouting sample, which consisted of **twenty five** questionnaires, through measuring the correlation coefficients between each paragraph in one field and the whole filed. Tables No. (3.7) below shows the correlation coefficient and p-value for each field items. As show in the table the p- Values are less than 0.05 or 0.01,so the correlation coefficients of this field are significant at $\alpha = 0.01$ or $\alpha = 0.05$, so it can be said that the paragraphs of this field are consistent and valid to be measure what it was set for.

Table(3.6) The correlation coefficient between each paragraph in the field and the whole field(Risks of input data)

No.	Statement	Pearson coefficient	p-value
1	Unintentional entry of data by staff	0.449	0.015
2	Intentional the input of data by staff	0.529	0.004
3	Unintentional destruction of data by staff	0.466	0.011
4	The deliberate destruction of data by staff	0.623	0.000
5	Data can be accessed quickly by staff	0.546	0.002
6	Can unauthorized persons access to data from outside the University	0.476	0.009
7	Enter virus to regulations of Islamic University	0.571	0.001

Table(3.7)The correlation coefficient between each paragraph in the field and the whole field(Risks of output data)

No.	**Statement**	**p-value**	Pearson **coefficient**
1	Distortion output of data	0.743	0.000
2	Generate output false / incorrect	0.628	0.000
3	Theft of data / information	0.556	0.002
4	To make unauthorized copies of outputs	0.635	0.000
5	Unauthorized disclosure of data by displayed on screens or printed on	0.707	0.000
6	Printing and distribution of information by unauthorized persons	0.760	0.000
7	Publications and distributed information error is directed to persons not authorized to receive a copy of distributed information	0.693	0.000
8	Delivery of sensitive documents to people who do not meet the terms of security for the purpose of tearing or disposal	0.562	0.002

Table(3.8)The correlation coefficient between each paragraph in the field and the whole field(Surrounding Technology Risks)

No.	Statement	p-value	Pearson coefficient
1	Penetrationoutside	0.719	0.000
2	Interception of data access from servers to users	0.651	0.000
3	State policy are reluctant to use modern technology	0.554	0.004
4	The blockade prevents the modern machines arrived to protect data and networks	0.645	0.001
5	The financial position of the University does not provide technology needs	0.673	0.000
6	Natural disasters such as fires and intentional disasters such as the Zionist bombing	0.574	0.003

Table(3.9)The correlation coefficient between each paragraph in the field and the whole field(the lack of experience and training risks)

No.	Statement	p-value	Pearson coefficient
1	The lack of the necessary expertise and adequate training and scientific background and skills required for the implementation of actions by the staff of the university	0.534	0.015
2	Not requiring employees to take regular leave	0.812	0.000
3	Insufficient attention to examine the career and vocational history for new staff	0.557	0.004
4	Lack of interest in the research of economic and social problems and psychological staff of the Islamic University	0.556	0.004
5	Lack of sufficient awareness among staff of the need to examine any programs or disks when introduced to new computers	0.649	0.000

Table(3.10)The correlation coefficient between each paragraph in the field and the whole field(the weakness of control procedure risks)

No.	Statement	p-value	Pearson coefficient
1	Weaknesses in the control system at the university and ineffective	0.537	0.006
2	The participation of staff in using the same passwords	0.616	0.001
3	Lack of segregation of duties and functions related to information systems and communications	0.533	0.006
4	The lack of specific policies and programs and written to the security of information and communication systems	0.571	0.003
5	Inadequate protection against the risks of computer viruses in the university	0.495	0.012
6	No accurate description of the functional and administrative structure which defines the responsibilities and powers of each person within the Islamic University - Gaza	0.649	0.000
7	There is no clear policy is forcing staff to change the password every time	0.483	0.014

Table(3.11)The correlation coefficient between each paragraph in the field and the whole field(Policies and procedures)

No.	Statement	p-value	Pearson coefficient
1	The university administration to issue special administrative decisions to avoid the risk of information security	0.537	0.006
2	The senior management of the University undertakes to apply information security	0.616	0.001
3	Relay information security management in the implementation of the protection measures required	0.566	0.003
4	The university administration set up special rules to protect the security of information and to punish violators of these rules staff	0.736	0.000

5	The information security management to develop a plan to protect a comprehensive and in-depth penetration include closing ports, and internal audit procedures and keep a backup copy of the information can be referenced when necessary	0.659	0.000
6	Applied information security management such as privacy, and avoid changing the unauthorized data, and availability of data at the specified time	0.700	0.000
7	The analysis of information security management information security risks, such as the expected return against the costs of countermeasures	0.706	0.000
8	The information security management by adopting information security policies regarding the selection of appropriate technology and its mechanism of action	0.771	0.000
9	The information security management installed technical protection methods such as firewalls and anti-virus and others	0.646	0.000
10	The information security management updates protection banger as changes in environment technology	0.745	0.000
11	The information security management analysis hacking incidents through the reports, and identify and describe the type of penetration	0.618	0.001
12	The information security management repelled breach when it occurs and the resulting fix bugs and does not recur	0.604	0.001
13	Benefit the university administration from the experience of universities in the world in the field of information security and communications	0.634	0.001
14	Are the students role in penetrating the system	0.486	0.008
15	Do repeat the hack from specific directions	0.678	0.000

4. Structure Validity of the Questionnaire

Structure validity is the second statistical test that used to test the validity of the questionnaire structure by testing the validity of each field and the validity of the whole questionnaire. It measures the correlation coefficient between one filed and all the fields of the questionnaire that have the same level of liker scale.

As shown in table No. (3.13), the significance values are less than 0.05 or 0.01, so the correlation coefficients of all the fields are significant at $\alpha = 0.01$ or $\alpha = 0.05$, so it can be said that the fields are valid to be measured what it was set for to achieve the main aim of the research

Table No. (3.12)Structure Validity of the Questionnaire

No.	Section	Pearson **correlation coefficient**	p-value
1	Risks of input data	0.701	0.000
2	Risks of output data	0.805	0.000
3	Surrounding Technology Risks	0.687	0.000
4	the lack of experience and training risks	0.742	0.000
5	the weakness of control procedure risks	0.651	0.000
6	Policies and procedures	0.679	0.000

Eighth : Reliability of the Research

Reliability of an instrument is the degree of consistency with which it measures the attribute it is supposed to be measuring . The test is repeated to the same sample of people on two occasions and then compares the scores obtained by computing a reliability coefficient. For the most purposes reliability coefficient above 0.7 are considered satisfactory. Period of two weeks to a month is recommended between two tests Due to complicated conditions that the contractors is facing at the time being, it was too difficult to ask them to responds to our questionnaire twice within short period. The statistician's explained that, overcoming the distribution of the questionnaire twice to measure the

reliability can be achieved by using Kronpakh Alph coefficient and Half Split Method through the SPSS software.

Ninth :Half Split Method

This method depends on finding Pearson correlation coefficient between the means of odd rank questions and even rank questions of each field of the questionnaire. Then, correcting the Pearson correlation coefficients can be done by using Spearman Brown correlation coefficient of correction. The corrected correlation coefficient (consistency coefficient) is computed according to the following equation :

Consistency coefficient = 2r/(r+1), where r is the Pearson correlation coefficient. The normal range of corrected correlation coefficient 2r/(r+1) is between 0.0 and + 1.0 As shown in Table No.(3.14), all the corrected correlation coefficients values are between 0.8085 and 0.8785 and the general reliability for all items equal 0.8696, and the significant (α) is less than 0.05 so all the corrected correlation coefficients are significance at α = 0.05. It can be said that according to the Half Split method, the dispute causes group are reliable.

Table (3.13)Split-Half Coefficient method

No.	Section	person-correlation	Spearman-Brown Coefficient	Sig. (2-Tailed)
1	Risks of input data	0.7424	0.8521	0.000
2	Risks of output data	0.6926	0.8184	0.000
3	Surrounding Technology Risks	0.6785	0.8085	0.000

No.	Section	person-correlation	Spearman-Brown Coefficient	Sig. (2-Tailed)
4	the lack of experience and training risks	0.7832	0.8785	0.000
5	the weakness of control procedure risks	0.7143	0.8333	0.000
6	Policies and procedures	0.7693	0.8696	0.000
	All fields	0.7254	0.8408	0.000

Tenth :Cronbach's Coefficient Alpha

This method is used to measure the reliability of the questionnaire between each field and the mean of the whole fields of the questionnaire. The normal range of Cronbach's coefficient alpha value between 0.0 and + 1.0, and the higher values reflects a higher degree of internal consistency. As shown in Table No. (3.15) the Cronbach's coefficient alpha was calculated and the results were in the range from 0.8267and 0.8925, and the general reliability for all items equal 0.8633. This range is considered high; the result ensures the reliability of the questionnaire.

Table (3.14)for Reliability Cronbach's Alpha

No.	Section	No. of Items	Cronbach's Alpha
1	Risks of input data	7	0.8364
2	Risks of output data	8	0.8456

No.	Section	No. of Items	Cronbach's Alpha
3	Surrounding Technology Risks	6	0.8267
4	the lack of experience and training risks	5	0.8925
5	the weakness of control procedure risks	7	0.8513
6	Policies and procedures	15	0.8768
	All fields	48	0.8633

Eleventh : Statistical Manipulation:

To achieve the research goal, researcher used the statistical package for the Social Science (SPSS) for Manipulating and analyzing the data.

Twelve : Statistical methods are as follows:

1. Frequencies and Percentile
2. Alpha- Cronbach Test for measuring reliability of the items of the questionnaires
3. Person correlation coefficients for measuring validity of the items of the questionnaires.
4. spearman –Brown Coefficient
5. one sample t test
6. independent samples t test
7. one way ANOVA test
8. Scheffe Multiple Comparisons test

Chapter 4

Data Analysis and Discussion

First: Introduction

Second : One Sample K-S Test

Third :Fourth: Test of Hypothesis

First :Introduction:

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

Second : One Sample K-S Test

One Sample K-S test is used to identify if the data follow normal distribution or not, this test is considered necessary in case testing hypotheses as most parametric Test stipulate data to be normality distributed and this test used when the size of the sample are greater than 50. Results test as shown in table (4.1) , clarifies that the calculated p-value is greater than the significant level which is equal 0.05 (p-value. > 0.05thus it means that data follows normal distribution, and so parametric Tests must be used.

Table (4.1)One Sample K-S

No.	Section	No. of Items	Statistic	P-value
1	Risks of input data	7	0.585	0.884
2	Risks of output data	8	0.813	0.523
3	Surrounding Technology Risks	6	1.070	0.202
4	the lack of experience and training risks	5	0.634	0.816
5	the weakness of control procedure risks	7	0.856	0.456
6	Policies and procedures	15	0.795	0.552
	All fields	48	0.404	0.997

Third : Test of Hypothesis

1. Main Hypothesis (1):

There is a statistically significant effect at (α=0.05) of the security information and communication management factors on the security of information and communication management

a) Sub-hypothesis

H1a: There is a statistically significant effect at (α=0.05) of risks input data on the security of information and communication management

To test the hypothesis we use a one sample t test and the opinion of the respondent about **Risks of input data** ranked according to the weight mean as shown in Table No. (4.2) as follows:

Table No.(4.2)Risks of input data

No.	Sentence	Mean	standard deviation	Weight mean	t-value	P-value	rank
1	Unintentional entry of data by staff	3.16	1.156	63.21	1.040	0.303	2
2	Intentional the input of data by staff	2.59	1.233	51.79	-2.494	0.016	6
3	Unintentional destruction of data by staff	2.96	1.159	59.29	-0.231	0.819	3
4	The deliberate destruction of data by staff	2.59	1.398	51.79	-2.198	0.032	7
5	Data can be accessed quickly by staff	3.61	1.123	72.14	4.046	0.000	1
6	Can unauthorized persons access to data from outside the University	2.66	1.379	53.21	-1.841	0.071	5
7	Enter virus to regulations of Islamic University	2.77	1.362	55.36	-1.276	0.207	4
	All items	2.91	0.802	58.11	-0.881	0.382	

Critical value of **t** at df "55" and significance level 0.05 equal 2.0

1. In item No. (5) (Data can be accessed quickly by staff)the weight mean equal " 72.14%" and p-value equal " 0.000" which is less than 0.05, and ranked equal " 1".

2. In item No. (1) (Unintentional entry of data by staff) the weight mean equal " 63.21%" and p-value equal " 0.303" which is greater than 0.05, and ranked equal " 2".

3. In item No. (3) (Unintentional destruction of data by staff) the weight mean equal " 59.29%" and p-value equal " 0.819" which is greater than 0.05, and ranked equal " 3".

4. In item No. (7) (Enter virus to regulations of Islamic University) the weight mean equal " 55.36%" and p-value equal " 0.207" which is greater than 0.05, and ranked equal " 4".

5. In item No. (6) (Can unauthorized persons access to data from outside the University)the weight mean equal " 53.21%" and p-value equal " 0.071" which is greater than 0.05, and ranked equal " 5".

6. In item No. (5) (Intentional the input of data by staff)the weight mean equal " 51.79%" and p-value equal " 0.016" which is less than 0.05, and ranked equal " 6".

7. In item No. (4) (The deliberate destruction of data by staff)the weight mean equal " 51.79%" and p-value equal " 0.032" which is less than 0.05, and ranked equal " 7".

For general the results for all items of the field show that the average mean equal 2.91 **and the weight mean equal** 58.11% **which is less than " 60%" and the value of t test equal** 0.881 **which is less than the critical value which is equal 2.0 and the p-value equal 0.382 which is greater than 0.05, that means**

there is no statistically significant effect at (α=0.05) of Risks input data on the security of information and communication management**.**

The analysis of the questionnaire shows that there is no effect of input risks on ICT security where the general weight average is 58.11% , also there is no big difference where the weight average , data can be accessed quickly by staff ,that means the current security system may be classified as slightly secures and acceptable ,but need to some complexity toward security , **intentional entry of data by staff was** 51.79 **and this agree with obeidi,2010) research, where was a lot of risks and agreed with (van Niekerk and Von Solms,2010) ,where the research recommend that many processes needed to protect the information assets.It is proved that the IUG should prepare forms and clear standards rules to improve input data process.**

H1b: There is a statistically significant effect at (α=0.05) of risks output data on The security of information and communication management

To test the hypothesis we use a one sample t test and the opinion of the respondent about **Risks of output data** ranked according to the weight mean as shown in Table No. (4.3) as follows:

Table No.(4.3)Risks of output data

No.	Sentence	Mean	standard deviation	Weight mean	t-value	P-value	rank
1	Distortion output of data	2.68	1.046	53.57	-2.299	0.025	6
2	Generate output false / incorrect	2.34	1.210	46.79	-4.086	0.000	8
3	Theft of data / information	2.48	1.388	49.64	-2.792	0.007	7
4	To make unauthorized copies of outputs	2.88	1.389	57.50	-0.673	0.504	2
5	Unauthorized disclosure of data by displayed on screens or printed on	2.95	1.151	58.93	-0.348	0.729	1

6	Printing and distribution of information by unauthorized persons	2.82	1.350	56.43	-0.990	0.327	4
7	Publications and distributed information error is directed to persons not authorized to receive a copy of distributed information	2.84	1.318	56.79	-0.912	0.366	3
8	Delivery of sensitive documents to people who do not meet the terms of security for the purpose of tearing or disposal	2.73	1.355	54.64	-1.479	0.145	5
	All items	2.71	1.052	54.29	-2.033	0.047	

Critical value of **t** at df "55" and significance level 0.05 equal 2.0

1. In item No. (5) (Unauthorized disclosure of data by displayed on screens or printed on)the weight mean equal " 58.93%" and p-value equal " 0.729" which is greater than 0.05, and ranked equal " 1".

2. In item No. (4) (To make unauthorized copies of outputs)the weight mean equal " 57.50%" and p-value equal " 0.504" which is greater than 0.05, and ranked equal " 2".

3. In item No. (7) (Publications and distributed information error is directed to persons not authorized to receive a copy of distributed information).the weight mean equal " 56.79%" and p-value equal " 0.366" which is greater than 0.05, and ranked equal " 3".

4. In item No. (6) (Printing and distribution of information by unauthorized persons) the weight mean equal " 56.43%" and p-value equal " 0.327" which is greater than 0.05, and ranked equal " 4".

5. In item No. (8) (Delivery of sensitive documents to people who do not meet the terms of security for the purpose of tearing or disposal) the weight mean equal " 54.64%" and p-value equal " 0.145" which is greater than 0.05, and ranked equal " 5".

6. In item No. (1) (Distortion output of data) the weight mean equal " 53.57%" and p-value equal " 0.025" which is less than 0.05, and ranked equal " 6".

7. In item No. (3) (Theft of data / information)the weight mean equal " 49.64%" and p-value equal " 0.007" which is less than 0.05, and ranked equal " 7".

8. In item No. (2) (Generate output false / incorrect)the weight mean equal " 46.79%" and p-value equal " 0.000" which is less than 0.05, and ranked equal " 8".

For general the results for all items of the field show that the average mean equal 2.71 **and the weight mean equal** 54.29% **which is less than " 60%" and the value of t test equal** 2.033 **which is greater than the critical value which is equal 2.0 and the p- value equal** 0.047 **which is less than 0.05, that means**

There is no statistically significant effect at (α=0.05) of risks output data on the security of information and communication management

The analysis of the questionnaire shows that there is no effect of output risks on ICT security where the general weight average is 54.29% ,also there is no big difference where the weight average in Distortion output of data was 53.57% , generate output false / incorrect was 46.49 and Theft of data / information was 49.67 . In addition this also agrees with (Ashenden,2008)which suggest that to address the issue to look at skills needed to change organizational culture and identity of information security manager and effective communication between information security manage and end user and senior manager. It should be cleared that the classified document must be destroyed after used.

H1c: There is a statistically significant effect at (α=0.05) of surrounding on The security of information and communication management.

To test the hypothesis we use a one sample t test and the opinion of the respondent about Surrounding Technology Risks ranked according to the weight mean as shown in Table No. (4.4) as follows:

Table No.(4.4)Surrounding Technology Risks

No.	Sentence	Mean	standard deviation	Weight mean	t-value	P-value	rank
1	Penetration outside	3.29	1.385	65.71	1.544	0.128	4
2	Interception of data access from servers to users	3.39	1.155	67.86	2.546	0.014	3
3	State policy are reluctant to use modern technology	2.59	1.125	51.79	-2.733	0.008	6
4	The blockade prevents the modern machines arrived to protect data and networks	3.70	1.111	73.93	4.693	0.000	2
5	The financial position of the University does not provide technology needs	3.09	1.225	61.79	0.545	0.588	5
6	Natural disasters such as fires and intentional disasters such as the Israeli bombing	3.86	0.773	77.14	8.299	0.000	1
	All items	3.32	0.667	66.37	3.573	0.001	

Critical value of **t** at df "55" and significance level 0.05 equal 2.0

In item No. (6) (Natural disasters such as fires and intentional disasters such as the Zionist bombing)the weight mean equal " 77.14%" and p-value equal " 0.000" which is less than 0.05, and ranked equal " 1"

In item No. (4) (The blockade prevents the modern machines arrived to protect data and networks)the weight mean equal " 73.93%" and p-value equal " 0.000" which is less than 0.05, and ranked equal " 2"

In item No. (2) (Interception of data access from servers to users) the weight mean equal " 67.86%" and p-value equal " 0.014" which is less than 0.05, and ranked equal " 3"

In item No. (1) (Penetration outside) the weight mean equal " 65.71%" and p-value equal " 0.128" which is greater than 0.05, and ranked equal " 4"

In item No. (5) (The financial position of the University does not provide technology needs)the weight mean equal " 61.79%" and p-value equal " 0.588" which is greater than 0.05, and ranked equal " 5"

In item No. (3) (State policy are reluctant to use modern technology) the weight mean equal " 51.79%" and p-value equal " 0.008" which is less than 0.05, and ranked equal " 6"

For general the results for all items of the field show that the average mean equal 3.32 **and the weight mean equal** 66.37**% which is greater than " 60%" and the value of t test equal** 3.573 **which is greater than the critical value which is equal 2.0 and the p- value equal 0.001 which is less than 0.05, that means**

There is a statistically significant effect at (α=0.05) of surrounding on The security of information and communication management

Based on the test result shows that the impact of surrounding technology on ICT security significant which means that the system can be penetrate from outside this research agreed with (Hung,et,2010) which consider the characteristics of five dangerous threats such as Hackers, worms ,viruses, Trojan Horses and back door programs, which outside penetration tools , there is statistical significant relationship between the Risks on the surrounding technology and the level of system security from the point of view of respondents associated to natural disasters, fire, Israeli attack.

The blockade prevents the modern technology to secure the system significant and affect the ICT security where the weighted average was 73.93% .

H1d: There is a statistically significant effect at (α=0.05) of Lack experience and training on The security of information and communication management

To test the hypothesis we use a one sample t test and the opinion of the respondent about **the lack of experience and training risks** ranked according to the weight mean as shown in Table No. (4.5) as follows:

Table No.(4.5)the lack of experience and training risks

No.	Sentence	Mean	standard deviation	Weight mean	t-value	P-value	rank
1	The lack of the necessary expertise and adequate training and scientific background and skills required for the implementation of actions by the staff of the university	3.20	1.119	63.93	1.314	0.194	3
2	Not requiring employees to take regular leave	3.16	1.058	63.21	1.137	0.261	4
3	Insufficient attention to examine the career and vocational history for new staff	3.07	1.006	61.43	0.531	0.597	5
4	Lack of interest in the research of economic and social problems and psychological staff of the Islamic University	3.52	1.112	70.36	3.486	0.001	2
5	Lack of sufficient awareness among staff of the need to examine any programs or disks when introduced to new computers	3.61	1.107	72.14	4.106	0.000	1
	All items	3.31	0.725	66.21	3.209	0.002	

Critical value of **t** at df "55" and significance level 0.05 equal 2.0

1. In item No. (5) (Lack of sufficient awareness among staff of the need to examine any programs or disks when introduced to new computers)the weight mean equal " 72.14%" and p-value equal " 0.000" which is less than 0.05, and ranked equal " 1"

2. In item No. (4) (Lack of interest in the research of economic and social problems and psychological staff of the Islamic University)the weight mean equal " 70.36%" and p-value equal " 0.001" which is less than 0.05, and ranked equal " 2".

3. In item No. (1) (The lack of the necessary expertise and adequate training and scientific background and skills required for the implementation of actions by the staff of the university)the weight mean equal " 63.93%" and p-value equal " 0.194" which is greater than 0.05, and ranked equal " 3".

4. In item No. (2) (Not requiring employees to take regular leave)the weight mean equal " 63.21%" and p-value equal " 0.261" which is greater than 0.05, and ranked equal " 4"

5. In item No. (3) (Insufficient attention to examine the career and vocational history for new staff)the weight mean equal " 61.43%" and p-value equal " 0.597" which is greater than 0.05, and ranked equal " 5".

For general the results for all items of the field show that the average mean equal *3.31* ***and the weight mean equal*** *66.21%* ***which is greater than " 60%" and the value of t test equal*** *3.209* ***which is greater than the critical value which is equal 2.0 and the p-value equal 0.002 which is less than 0.05, that means***

There is a statistically significant effect at (α=0.05) of Lack experience and training on The security of information and communication management

The analysis shows that the effect of experience and training of staff significant with weighted average of 66.2% which means that the IUG should support train the staff to be aware on security issues which affect the ICT security also shows that the lack of the staff awareness of the need to examine any storage media will enter and used by the system where the weighted average was 72% which challenge the management to train the staff how to deal with entering of using data of the system and put the management on their responsibilities to research the social and economic situation of their staff which shows lack and in satisfaction on the issues . it is proved that the IUG should consider the training as one of the important factors that contribute in improve the management and security process. In addition this also agrees with(kraemer,et,2009)which conclude that there is presence of the correlation between organizational and human factors technical issues and information security. Also agreed with (shaw ,et,2009) research which conclude that the learners who have high level of awareness and understanding enable them to improve the level of protection.

H1e: There is a statistically significant effect at (α=0.05) of weakness of control procedure on The security of information and communication management

To test the hypothesis we use a one sample t test and the opinion of the respondent about **the weakness of control procedure risks** ranked according to the weight mean as shown in Table No. (4.6) as follows:

Table No.(4.6)the weakness of control procedure risks

No.	Sentence	Mean	standard deviation	Weight mean	t-value	P-value	rank
1	Weaknesses in the control system at the university and ineffective	2.71	0.967	54.29	-2.211	0.031	6
2	The participation of staff in using the same passwords	3.29	1.004	65.71	2.130	0.038	2
3	Lack of segregation of duties and functions related to information systems and communications	3.20	0.999	63.93	1.472	0.147	3
4	The lack of specific policies and programs and written to the security of information and communication systems	3.09	1.066	61.79	0.627	0.534	4
5	Inadequate protection against the risks of computer viruses in the university	2.70	1.159	53.93	-1.961	0.055	7
6	No accurate description of the functional and administrative structure which defines the responsibilities and powers of each person within the Islamic University – Gaza	2.84	1.075	56.79	-1.119	0.268	5
7	There is no clear policy is forcing staff to change the password every time	3.30	1.159	66.07	1.961	0.020	1
	All items	3.02	0.670	60.36	0.199	0.843	

Critical value of **t** at df "56" and significance level 0.05 equal 2.0

1. In item No. (7) (There is no clear policy is forcing staff to change the password every time)the weight mean equal " 66.07%" and p-value equal " 0.055" which is greater than 0.05, and ranked equal " 1"

2. In item No. (2) (The participation of staff in using the same passwords)the weight mean equal " 65.71%" and p-value equal " 0.038" which is less than 0.05, and ranked equal " 2"

3. In item No. (3) (Lack of segregation of duties and functions related to information systems and communications)the weight mean equal " 63.93%" and p-value equal " 0.147" which is greater than 0.05, and ranked equal " 3"

4. In item No. (4) (The lack of specific policies and programs and written to the security of information and communication systems) the weight mean equal " 61.79%" and p-value equal " 0.534" which is greater than 0.05, and ranked equal " 4"

5. In item No. (6) (No accurate description of the functional and administrative structure which defines the responsibilities and powers of each person within the Islamic University - Gaza)the weight mean equal " 56.79%" and p-value equal " 0.268" which is greater than 0.05, and ranked equal " 5"

6. In item No. (1) (Weaknesses in the control system at the university and ineffective)the weight mean equal " 54.29%" and p-value equal " 0.031" which is less than 0.05, and ranked equal " 6"

7. In item No. (5) (Inadequate protection against the risks of computer viruses in the university)the weight mean equal " 53.93%" and p-value equal " 0.055" which is greater than 0.05, and ranked equal " 7"

For general the results for all items of the field show that the average mean equal 3.02 **and the weight mean equal** 60.36**% which is greater than " 60%" and the value of t test equal** 0.199 **which is less than the critical value which is equal 2.0 and the p- value equal 0.843 which is greater than 0.05, that means**

There is no statistically significant effect at (α=0.05) of weakness of control procedure on The security of information and communication management

The analysis of the questionnaire shows that there is effect of weakness control procedure risks on ICT security where the general weight average is 60.36% ,also there is no clear policy forcing the staff to change the password periodically where the weight average was 66.7%, and this agree with (Houria Al-Sharif,2006) which show that the participation of the staff in the use of the same password make the system unsecure. Also this research disagreed with (Zidane and Hamo,2010) where the research found that there is a lack of legislations and laws regulating the banking system in the internet technology, the justification of this is the requirement and legislation and laws control of internet security still under development and needs a more awareness and development, moreover the internet security face more outside threats than internal systems.

H1f: **There is a statistically significant effect at (α=0.05) of Policies and procedures on The security of information and communication management**

To test the hypothesis we use a one sample t test and the opinion of the respondent about **Policies and procedures** .Table No.(4.7) shows the heights three items according to the weight mean as follows:

Table No.(4.7)Policies and procedures

No.	Sentence	Mean	standard deviation	Weight mean	t-value	P-value
1	The university administration to issue special administrative decisions to avoid the risk of information security	3.77	0.786	75.36	7.310	0.000
2	The senior management of the University undertakes to apply information security	3.77	0.934	75.36	6.152	0.000
3	Relay information security management in the implementation of the protection measures required	3.66	0.859	73.21	5.758	0.000
4	The university administration set up special rules to protect the security of information and to punish violators of these rules staff	3.64	1.017	72.86	4.731	0.000
5	The information security management to develop a plan to protect a comprehensive and in-depth penetration include closing ports, and internal audit procedures and keep a backup copy of the information can be referenced when necessary	3.88	0.833	77.50	7.865	0.000
6	Applied information security management such as privacy, and avoid changing the unauthorized data, and availability of data at the specified time	3.82	0.690	76.43	8.904	0.000
7	The analysis of information security management information security risks, such as the expected return against the costs of countermeasures	3.27	0.842	65.36	2.381	0.021

Continue : Table No.(4.7)Policies and procedures

8	The information security management by adopting information security policies regarding the selection of appropriate technology and its mechanism of action	3.46	0.873	69.29	3.979	0.000
9	The information security management installed technical protection methods such as firewalls and anti-virus and others	3.95	0.818	78.93	8.654	0.000
10	The information security management updates protection banger as changes in environment technology	3.84	0.848	76.79	7.406	0.000
11	The information security management analysis hacking incidents through the reports, and identify and describe the type of penetration	3.80	0.818	76.07	7.348	0.000
12	The information security management repelled breach when it occurs and the resulting fix bugs and does not recur	3.80	0.980	76.07	6.135	0.000
13	Benefit the university administration from the experience of universities in the world in the field of information security and communications	3.66	0.900	73.21	5.493	0.000
14	Are the students role in penetrating the system	3.71	0.909	74.29	5.881	0.000
15	Do repeat the hack from specific directions	3.27	0.981	65.36	2.042	0.046
	All items	3.69	0.431	73.74	11.939	0.000

Critical value of **t** at df "55" and significance level 0.05 equal 2.0

1. In item No. (9) the weight mean equal " 78.93%" and p-value equal " 0.000" which is less than 0.05, that means (The information security management installed technical protection methods such as firewalls and anti-virus and others).

2. In item No. (5) the weight mean equal " 77.50%" and p-value equal " 0.000" which is less than 0.05, that means (The information security management to develop a plan to protect a comprehensive and in-depth penetration include closing ports, and internal

audit procedures and keep a backup copy of the information can be referenced when necessary).

3. In item No. (10) the weight mean equal " 76.79%" and p-value equal " 0.000" which is less than 0.05, that means (The information security management updates protection banger as changes in environment technology).

   And the lowest three items according to the weight mean as follows

4. In item No. (8) the weight mean equal " 69.29%" and p-value equal " 0.000" which is less than 0.05, that means (The information security management by adopting information security policies regarding the selection of appropriate technology and its mechanism of action).

5. In item No. (7) the weight mean equal " 65.36%" and p-value equal " 0.021" which is less than 0.05, that means (The analysis of information security management information security risks, such as the expected return against the costs of countermeasures).

6. In item No. (15) the weight mean equal " 65.36%" and p-value equal " 0.046" which is less than 0.05, that means (Do repeat the hack from specific directions).

For general the results for all items of the field show that the average mean equal 3.69 **and the weight mean equal** 73.74**% which is greater than " 60%" and the value of t test equal** 11.939 **which is greater than the critical value which is equal 2.0 and the p- value equal 0.000 which is less than 0.05, that means**

there is a statistically significant effect at (α=0.05) of Policies and procedures on The security of information and communication management

The analysis of the questionnaire shows that there is significant effect of policies and procedure on ICT security where the weighted average was 73.4% and shows that there is penetrate from special directions by weighted average 65% and IUG to secure the ports by firewalls .and this research agree with (George,2011) research which argued that Threats and vulnerabilities regarding information security are pushing organizations to better protect their valuable information and resources by using an information security management system. Also agreed with (Badi,2010) research which shows the university should follow a clear policy about the mechanism to deal with some of the risks and anticipated threats to system.

Also the findings this research agreed with (Knapp,et,2009) information security policies are a necessary foundation of organizational security program.

Main Hypothesis (1):

There is a statistically significant effect at (α=0.05) of The security information and communication management factors on The security of information and communication management

The research used a one sample t test to test the opinion of the respondent about the information security management in light of network technologies and the results in Table No. (4.8) shows that the average mean for all fields equal 3.23 and the weight mean equal 64.56% which is less than " 60%" and the absolute value of t test equal 4.082 which is greater than the critical value which is equal 2.0 and the p- value equal 0.000 which is less than 0.05, that mean there is a statistically significant effect at (α=0.05) of The security information and communication management factors on The security of information and communication management

Table(4.8) All fields

No.	**Field**	**Mean**	**standard deviation**	**Weight mean**	**t-value**	**P-value**
1	Risks of input data	2.91	0.802	58.11	-0.881	0.382
2	Risks of output data	2.71	1.052	54.29	-2.033	0.047
3	Surrounding Technology Risks	3.32	0.667	66.37	3.573	0.001
4	the lack of experience and training risks	3.31	0.725	66.21	3.209	0.002
5	the weakness of control procedure risks	3.02	0.670	60.36	0.199	0.843
6	Policies and procedures	3.69	0.431	73.74	11.939	0.000
	All fields	3.23	0.418	64.56	4.082	0.000

Critical value of **t** at df "55" and significance level 0.05 equal 2.0

2. Main Hypothesis (2)

H1: There is a significant difference among the respondents' toward (Information Security and Communications Management in light of Networks Technology) due to demographic characters (Gender, age, experience, Job title, Qualifications)

And these Hypothesis divided into sub Hypotheses as follows:

There is a significant difference among the respondents' toward (Information Security and Communications Management in light of Networks Technology) due to Qualifications.

To test the question we use the one way ANOVA test and the result illustrated in table no.(4.9) which shows the following results: the p-value equal 0.544 which is greater than 0.05 and the value of F test equal 0.721 which is less than the value of critical value which is equal 2.78, that's means There is no significant difference among the respondents' toward (Information Security and Communications Management in light of Networks Technology) due to Qualifications

Table (4.9) One way ANOVA test for difference among the respondents' toward (Information Security and Communications Management in light of Networks Technology) due to Qualifications

Research problem	Source	Sum of Squares	df	Mean Square	F value	Sig.(P-Value)
Information Security and Communications Management in light of Networks Technology	Between Groups	0.384	3	0.128	0.721	0.544
	Within Groups	9.229	52	0.177		
	Total	9.613	55			

Critical value of F at df "3,52" and significance level 0.05 equal 2.78

this result indicates that there are no differences among the respondents in their opinions over the research 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 research fields attributed to their qualification, which means that whatever the respondent qualification is, will nor differ from each other because the basic knowledge and principle of the security will be constant against security.

There is a significant difference among the respondents' toward (Information Security and Communications Management in light of Networks Technology) due to Gender

To test the hypothesis we use the Independent Samples Test and the result illustrated in table no.(4.10) which shows the following results: the p-value equal 0.848 which is greater than 0.05 and the absolute value of T test equal 0.193 which is less than the value of critical value which is equal 2.0, that's means There is no significant difference among the respondents' toward (Information Security and Communications Management in light of Networks Technology) due to Gender

Table No.(4.10) Independent Samples Test for difference among the respondents' toward (Information Security and Communications Management in light of Networks Technology) due to Gender

Research problem	Gender	N	Mean	Std. Deviation	T	P-value
Information Security and Communications Management in light of Networks Technology	Male	45	3.223	0.369	-0.193	0.848
	female	11	3.250	0.600		

Critical value of **t** at df "54" and significance level 0.05 equal 2.0

There is a significant difference among the respondents' toward (Information Security and Communications Management in light of Networks Technology) due to age.

To test the question we use the one way ANOVA test and the result illustrated in table no.(4.11) which shows the following results: the p-value equal 0.088 which is greater than 0.05 and the value of F test equal 2.304 which is less than the value of critical value which is equal 2.78 , that's means There is no significant difference among the respondents' toward (Information Security and Communications Management in light of Networks Technology) due to age

Table No.(4.11)One way ANOVA test for difference among the respondents' toward (Information Security and Communications Management in light of Networks Technology) due to age

Research problem	Source	Sum of Squares	df	Mean Square	F value	Sig.(P-Value)
Information Security and Communications Management in light of Networks Technology	Between Groups	1.128	3	0.376	2.304	0.088
	Within Groups	8.485	52	0.163		
	Total	9.613	55			

Critical value of F at df "3,52" and significance level 0.05 equal **2.78**

According to this result ―There are no significant statistical differences at level ($\alpha = 0.05$) among the respondents in their opinions over the research fields attributed to their age.

There is a significant difference among the respondents' toward (Information Security and Communications Management in light of Networks Technology) due to Job title

Table No.(4.12)One way ANOVA test for difference among the respondents' toward (Information Security and Communications Management in light of Networks Technology) due to Job title

Research problem	Source	Sum of Squares	df	Mean Square	F value	Sig.(P-Value)
Information Security and Communications Management in light of Networks Technology	Between Groups	0.585	2	0.293	1.718	0.189
	Within Groups	9.028	53	0.170		
	Total	9.613	55			

Critical value of F at df "2,53" and significance level 0.05 equal 3.17

To test the question we use the one way ANOVA test and the result illustrated in table no.(4.12) which shows the following results: the p-value equal 0.189 which is greater than 0.05 and the value of F test equal 1.718 which is less than the value of critical value which is equal 3.17, that's means There is no significant difference among the respondents' toward (Information Security and Communications Management in light of Networks Technology) due to Job title

There is a significant difference among the respondents' toward (Information Security and Communications Management in light of Networks Technology) due to experience.

Table No.(4.13)One way ANOVA test for difference among the respondents' toward (Information Security and Communications Management in light of Networks Technology) due to experience

Research problem	Source	Sum of Squares	df	Mean Square	F value	Sig.(P-Value)
Information Security and Communications Management in light of Networks Technology	Between Groups	1.406	3	0.469	2.969	0.040
	Within Groups	8.208	52	0.158		
	Total	9.613	55			

Critical value of F at df "3,52" and significance level 0.05 equal 2.78

Table No.(4.14)Scheffe Multiple Comparisons test

Mean Difference	5 years and less	6 to 10 years	11 to 15 years	16 years and more
5 years and less		0.211	0.454*	0.229
6 to 10 years	-0.211		0.243	0.018
11 to 15 years	-0.454*	-0.243		-0.225
16 and more	-0.229	-0.018	0.225	

* The mean difference is significant at the .05 level

To test the question we use the one way ANOVA test and the result illustrated in table no.(4.13) which shows the following results: the p-value equal 0.040 which is less than 0.05 and the value of F test equal 2.969 which is greater than the value of critical value which is equal 2.78 , that's means There is a significant difference among the respondents 'toward (Information Security and Communications Management in light of Networks Technology) due to experience, and Scheffe Multiple Comparisons test table no.(28) show that there in a difference between " 5 years and less " , and "11 to 15 years " , and the difference in favor of "5 years and less" This result indicates that there are differences among the respondents in their opinions about these research fields with regard to the experience variable. This result agrees with the research of Alla aldeen (2013).

Chapter 5

CONCLUSIONS AND ECOMMENDATIONS

First: The Result

Third: Recommendations

Third : Further Research

First: The Result

The research reached several results :

1. There is statistical significant relationship between the risks on the surrounding technology and the level of system security from the point of view of the research population associated with natural disasters, fire, and Israeli attacks.
2. The impact of the surrounding technology on ICT security is significant which means that the system can be penetrated from outside.
3. The blockade prevents the imports of modern technology equipment to secure the system.
4. According to the research findings , the questionnaire respondents the research concludes that there is lack of staff experience and training in the field of updated security programs , policies and procedures. And there is dissatisfaction among the staff in the field of training specially in economic and social situation.
5. The research shows the risks associated with poor control procedures from the view point of the respondents in the two elements are: the participation of the staff in using the same password and there is no clear policy forcing the staff to change the password periodically.
6. Intercept and access data from servers to users' computers, because of the lack of knowledge of the mechanisms and their means of delivery, which requires improving access mechanisms.
7. Lack of adequate awareness among employees of the need to examine the new magnetic disks or programs when introduced to computers.

8. University administration benefit from the experience of international companies in the field of information security and communications.
9. Differences among the research respondents' opinions: There are no significant statistical differences at level ($\alpha = 0.05$) among the respondents in their opinions about the research fields attributed to gender, age, level of qualification, specialization and the Governmental Institution.
10. There are significant statistical differences at level ($\alpha = 0.05$) among the respondents in their opinions about the research fields attributed to experience .

Second : Recommendations

1. The IUG should prepare forms and clear standards rules to improve input data process.
2. The issue to look at skills needed to change organizational culture and identity of information security manager and effective communication between information security manage and end user and senior manager. It should be clear that the classified document must be destroyed after use.
3. Reduce the risk of controls through the use of expertise and best practices in improving the levels of control procedures.
4. Monitor the communications of IUG to keep confidential information that is often easy to access and penetrate, by developing general policy of protecting the security of information which clarify that the important information used by the staff ,then to be destroyed after every use.
5. The senior management of IUG should be committed to the security program and support of information systems security continuously.
6. The information technology department responsible for the security of information systems should be provided with qualified staff with sufficient experience in information systems security.
7. Give interest in information security to IUG through the components of the networking technology and this to be improved continuously.

8. The research recommends to train all employees to be more aware of security issues related to the system by clarifying the mechanisms to maintain data.
9. Develop procedures and policies to force the authorized employees "who have the authority to access and modify the data of the system", to change their password periodically. Moreover this model should be monitored and controlled to ensure that the system is secured and avoid stealing password.
10. The research recommends that not to allow the use of different kinds of storage media thereby to reduce the entry of virus into their systems in addition to do continuous updating of the antivirus software used by the university and set controls on the website to reduce the breakthroughs that could occur.
11. The research recommends that the IUG to hold and join international conferences regarding the ICT security, and to learn from other experiences worldwide.

Fourth: Further Research

1. Raising awareness of chief executive officers of small businesses in information security management in Palestine.
2. The impact of training and education on information security and communications.

References

Book

1. Ashenden, Debi, (2008), "Information Security management: A human challenge?", Information Security Technical Report, Vol.13, No.4: 195-201.
2. John&Hobo, (2009.)," WIRELESS SENSOR NETWORKS A Networking Perspective",Published simultaneously in Canada
3. Huang, Ding-Long: Rau, Pei-Luen Patrick &Salvendy, Gavriel, (2010), "Perception of information security", Behaviour& Information Technology, Vol. 29, No. 3, May-June: 221-232.
4. Humphreys, Edward, (2008), "Information security management standards: Compliance, governance and risk management", Information security Technical Report, Vol. 13, No.4: 247-255.
5. Hallberg, Bruce A. (2009). Networking: a beginner's guide. McGraw-Hill Professional. pp. 49–52
6. Kritzinger, E & Smith, E. (2008), "Information security management: An information security retrieval and awareness model for industry", Computer & Security, Vol.27, No. 5-6: 224-231.
7. Knapp, Kenneth J: Franklin, Morris: Thomas E. Marshall & Terry Anthony Byrd, (2009), "Information security policy: An organizational-level process model", Computer & Security, Vol. 28, No.7: 493-508.

8. Kraemer, Sara; Carayon, Pascale & Clem, John, (2009), "Human and organizational factors in computer and information security: Pathways to vulnerabilities", Computer & Security, Vol. 28, No. 7: 509-520.
9. Van Niekerk, J.F & Von Solms, R, (2010), "Information security culture: A management perspective", Computer & Security, Vol. 29: 476-486.

Master Thesis

1. Alaa Al-Deen,(2013),” Information Security Management for Strategic and ffective Implementation of e-Management: a case research in the Governmental Institutions in Gaza”held in Islamic university during Jan.2013.

2. Badi, Walid Salem (2010), "The fact of the security of information systems in the Omani libraries: a case research on the main library at Sultan Qaboos University," Sixth Conference of the Association of Library and Information Saudi Arabia, held in Riyadh during the period 6-7 April.

3. Houria Al-Sharif, (2006)," Threats that affect computerized accounting information systems",Case study of the banks in Gaza Strip – Palestine

4. Laudon, K &Laudon, J., (2010), "Management Information Systems", 11thed, Prentice Hall Int, Inc.

5. Swaminathan, P. Sekar., 2012)."Information and Communication Technology (ICT) and Society". International Journal of Computer Applications. Volume 1. 16-19

6. Obeidi, Hadeel Shawkat (2010), "The security of information and communication technology: a research of user awareness in the Kingdom of Bahrain," the Sixth

Conference of Library and Information Association Arabia, held in Riyadh during the 6-7 April.

7. Richard Y. K. Fung, (2008) , "Knowledge-Centric Information Security", International Conference on Security Technology, IEEE

8. Sultan, Abraham, (2009), "Management Information Systems: Systems Approach", University House for printing, publishing and distribution, Alexandria: Cairo.

9. Shaw, R.S; Charlie C. Chen; Albert L. Harris &Hui-Jou Huang, (2009), "The impact of information richness on information security awareness training effectiveness', Computers & Education, Vol. 52, No. 1: 92-100.

10. Siponen, Mikko & Willison, Robert, (2009), "Information security management standards: Problems and solutions", Information & Management, Vol. 46, No.5: 267-270.

11. Zidane and hamo (2010), "banking information security requirements in the online environment," the Sixth Conference of Library and Information Association Arabia, held in Riyadh during the 6-7 April

Papers and Articles

1. Barney Glover,(2011)." Information and Communication Technologies Security Policy ",the Charles Darwin University .
2. Fontaine Xavier and Katsunori Yamada, 2011. "Envy and Hope: Relevant Others' Consumption and Subjective Well-being in Urban India," PSE Working Papers hal-00616993, HAL
3. International Conferenece on EGovernance & Cloud Computing Sevices(EGov .2012)
4. Lugano, G., 2008. Mobile social networking in theory and practice.
5. ISO/IEC 27001. (2005). Information technology -- Security techniques -- Information security management systems – Requirements. ISO/IEC 27001:2005 International Organization for Standardization and International Electro technical Commission.
6. ISO/IEC 27002. (2005). Information technology -- Security techniques -- Code of practice for information security management. ISO/IEC 27002:2005. International Organization Standardization and International Electro technical Commission.
7. ITU (2008). ICTs for e-Environment- Guidelines for Developing Countries, with a Focus on Climate Change. ICT Applications and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunication Development Sector. Geneva.
8. Vasile G, (2012): ." Management International Communication And Information System", University of Craiova ,Mircea Alexandru Journal: , Seria Stiinte Economice ISSN 1584-2339 Volume: 22; Issue: 2; Start page: 81; Date: 2012 "
9. Tara, Zbibi, (2006), "The security of information and information systems," www.alrakameiat.com

Web sites

1. NCIHST.(2010). PSG College of Technology, Coimbatore
2. Computing Services Information Security Office (http://www.cmu.edu/iso/aware/presentation/tepperphd.pdf
3. PCMAG.com.(2009).http://www.pcmag.com/encyclopedia_term/0,2542,t=Smartphone&i=51537,00.asp"
4. IBM Internet Security Systems X-Force_. Mid-year trend statistics,www-304.ibm.com/businesscenter/cpe/download/183714/IBM_XFORCE_H1_2000.pdf; 2009
5. San Diego.(2013) "Communications and Information Security Symposium, ICNC 2013 http://www.conf-icnc.org/2013
3. Top 10 information security threats for 2010 according to PerimeterE-Security. (http://www.net-security.org)
6. http://www.iug.edu.ps

APPENDIX (A)

Questionnaire Arbitrators

No.	Name	Description
1	Dr. Issam Al-Buhaisi	Islamic University of Gaza
2	Dr. Rushdi Wadi	Islamic University of Gaza
3	Dr. Nafez Barkat	Islamic University of Gaza
4	Dr. Hosam Alnajar	Islamic University of Gaza
5	Dr. Faris Abu Maamar	Islamic University of Gaza
6	Eng. Hani Abu amer	Islamic University of Gaza
7	Eng. Nail Abo Rass	IT department at IUG
8	Dr. Alaa Alhaless	IT department at IUG
9	Dr. Iyad Elagha	IT department at IUG
10	Dr. Ashraf Thabet	IT department at IUG

Questionnaire

Dear Sir or Madam

Researcher aims to research titled "information security management in light of network technologies: a case research at the Islamic University of Gaza, where the research aims to manage information security in light of network technologies.

Please answer the questions of the questionnaire and borrow the best of your knowledge. Since your cooperation and your interest in the courtesy borrow the paragraphs of the resolution accurately and objectively, and reflect the reality of the case research variables in the Islamic University-Gaza will be important in the success of the research.

We trust your opinions and views will be respected and appreciated

Researcher

Raed Altoom
0599529093

General Information

1. Degree

☐ Diploma ☐ B.Sc. ☐ M.Sc. ☐ Ph.D.

2. Gender

☐ Male ☐ Female

3. Age

☐ Less than 25 years ☐ 25 to 34 years

☐ 35 to 44 years ☐ more than 45 years

4. Job title

☐ Director of the Department ☐ head of section

☐ Officer in the Department of Information Technology

5. number of experience years in the Current Position

☐ 5 years and less ☐ 6 to 10 years

☐ 11 to 15 years ☐ 16 and more

level	Strongly Agree	Agree	Neutral	Disagree	StronglyDisagree
Scale	SA	A	N	D	SD

Questionnaire

NO	Statement	Answer alternatives				
		SA	A	N	D	DA
a) Risks of input data						
1	Unintentional entry of data by staff					
2	Intentional the input of data by staff					
3	Unintentional destruction of data by staff					
4	The deliberate destruction of data by staff					
5	Data can be accessed quickly by staff					
6	Can unauthorized persons access to data from outside the University					
7	Enter virus to regulations of Islamic University					
b) Risks of output data						
8	Distortion output of data					
9	Generate output false / incorrect					
10	Theft of data / information					
11	To make unauthorized copies of outputs					
12	Unauthorized disclosure of data by displayed on screens or printed on					
13	Printing and distribution of information by unauthorized persons					
14	Publications and distributed information error is directed to persons not authorized to receive a copy of distributed information					
15	Delivery of sensitive documents to people who do not meet the terms of security for the purpose of tearing or disposal					
c) Surrounding Technology Risks						
16	Penetration outside					
17	Interception of data access from servers to users					
18	State policy are reluctant to use modern technology					
19	The blockade prevents the modern machines arrived to protect data and networks					
20	The financial position of the University does not provide technology needs.					

NO	Statement	SA	A	N	D	SD
21	Natural disasters such as fires and intentional disasters such as the Israeli bombing					
d) the lack of experience and training risks						
22	The lack of the necessary expertise and adequate training and scientific background and skills required for the implementation of actions by the staff of the university					
23	Not requiring employees to take regular leave					
24	Insufficient attention to examine the career and vocational history for new staff					
25	Lack of interest in the research of economic and social problems and psychological staff of the Islamic University					
26	Lack of sufficient awareness among staff of the need to examine any programs or disks when introduced to new computers					
e) the weakness of control procedure risks						
27	Weaknesses in the control system at the university and ineffective					
28	The participation of staff in using the same passwords					
29	Lack of segregation of duties and functions related to information systems and communications					
30	The lack of specific policies and programs and written to the security of information and communication systems					
31	Inadequate protection against the risks of computer viruses in the university					
32	No accurate description of the functional and administrative structure which defines the responsibilities and powers of each person within the Islamic University - Gaza					
33	There is no clear policy is forcing staff to change the password every time					
f) Policies and procedures						
34	The university administration to issue special administrative decisions to avoid the risk of information security					
35	The senior management of the University undertakes to apply information security					
36	Relay information security management in the implementation of the protection measures required					
37	The university administration set up special rules to protect the security of information and to punish violators of these rules staff					
38	The information security management to develop a plan to protect a comprehensive and in-depth penetration include					

	closing ports, and internal audit procedures and keep a backup copy of the information can be referenced when necessary					
39	Applied information security management such as privacy, and avoid changing the unauthorized data, and availability of data at the specified time					
40	The analysis of information security management information security risks, such as the expected return against the costs of countermeasures					
41	The information security management by adopting information security policies regarding the selection of appropriate technology and its mechanism of action					
42	The information security management installed technical protection methods such as firewalls and anti-virus and others					
43	The information security management updates protection banger as changes in environment technology					
44	The information security management analysis hacking incidents through the reports, and identify and describe the type of penetration					
45	The information security management repelled breach when it occurs and the resulting fix bugs and does not recur					
46	Benefit the university administration from the experience of universities in the world in the field of information security and communications					
47	Are the students role in penetrating the system					
48	Do repeat the hack from specific directions					

أداة الدراسة (الاستبانة)

الأخ الكريم/الأخت الكريمة ..... حفظه/ها الله

يهدف الباحث القيام بدراسة بعنوان " إدارة أمن المعلومات والاتصالات في ضوء تكنولوجيا الشبكات : **دراسة حالة على الجامعة الإسلامية- غزة**"، حيث تهدف الدراسة إلى إدارة أمن المعلومات والاتصالات في ضوء تكنولوجيا الشبكات.

برجاء الإجابة عن أسئلة الاستبانة كافة، وأن تجيب بأفضل ما لديك من معلومات. حيث أن تعاونكم واهتمامكم في التلطف بالإجابة عن فقرات الاستبانة بدقة وموضوعية، وبالشكل الذي يعكس واقع حال متغيرات الدراسة في الجامعة الإسلامية – غزة سيعد مهماً في نجاح الدراسة.

نحن نثق بآرائكم وستكون هذه الآراء موضع اعتزاز وتقدير

الباحث

رائد التوم

0599529093

الخصائص الشخصية:

المؤهل العلمي:

☐ دبلوم ☐ بكالوريوس

☐ ماجستير ☐ دكتوراه ☐ غير ذلك

الجنس:

☐ ذكر ☐ أنثى

العمر:

☐ أقل من 25 سنة ☐ من 25-34 سنة

☐ من 35-44 سنة ☐ 45 سنة فأكثر

المركز الوظيفي:

☐ مدير دائرة ☐ موظف في قسم تكنولوجيا المعلومات

☐ رئيس قسم

عدد سنوات الخدمة في الوظيفة الحالية:

☐ 5 سنوات فأقل ☐ من 6-10 سنوات

☐ من 11-15 سنة ☐ أكثر من 16 سنة

ت	الفقرة	بدائل الإجابة				
		موافق بشدة	موافق	محايد	معارض	معارض بشدة
(أ)	**مخاطر إدخال البياناتRisks of input data**					
1	الإدخال غير المتعمد لبيانات غير سليمة بواسطة الموظفين.					
2	الإدخال المتعمد لبيانات غير سليمة بواسطة الموظفين.					
3	التدمير غير المتعمد للبيانات بواسطة الموظفين.					
4	التدمير المتعمد للبيانات بواسطة الموظفين.					
5	يمكن الوصول إلي البيانات بشكل سريع بواسطة الموظفين					
6	يمكن لأشخاص غير مخولين بالدخول إلي البيانات من خارج الجامعة.					
7	إدخال فيروس للأنظمة المعمول بها في الجامعة الإسلامية					
(ب)	**مخاطر إخراج البياناتRisks of output data**					
8	تشويه المخرجات من البيانات.					
9	توليد مخرجات زائفة/ غير صحيحة.					
10	سرقة البيانات/ المعلومات					
11	عمل نسخ غير مصرح بها من المخرجات					
12	الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق.					
13	طبع وتوزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك.					

ت	الفقرة	بدائل الإجابة				
		موافق بشدة	موافق	محايد	معارض	معارض بشدة
14	المطبوعات والمعلومات الموزعة يتم توجيها خطأ إلى أشخاص غير مخول لهم في استلام نسخة منها.					
15	تسليم الوثائق الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها.					
(ت)	**مخاطر التكنولوجيا المحيطة Surrounding Technology Risks**					
16	الاختراقات الخارجية.					
17	اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين.					
18	سياسة الدولة تحجم من استخدام التكنولوجيا الحديثة					
19	الحصار يمنع وصل أجهزة حديثة من شأنها حماية البيانات و الشبكات					
20	الوضع المالي للجامعة لا يوفر الاحتياجات التكنولوجية					
21	الكوارث الطبيعية مثل الحرائق والكوارث المتعمدة مثل القصف الصهيوني					
(ث)	**مخاطر عدم وجود الخبر و التدريب the lack of experience and training risks**					
22	عدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الأعمال من قبل موظفي الجامعة .					
23	عدم إلزام الموظفين بأخذ إجازتهم الدورية.					
24	عدم الاهتمام الكافي بفحص التاريخ الوظيفي والمهني للموظفين الجدد.					

ت	الفقرة	بدائل الإجابة				
		موافق بشدة	موافق	محايد	معارض	معارض بشدة
25	عدم الاهتمام بدراسة المشاكل الاقتصادية والاجتماعية والنفسية لموظفي الجامعة الإسلامية.					
26	عدم الوعي الكافي لدى الموظفين بضرورة فحص أي برامج أو أقراص الممغنطة الجديدة عند إدخالها إلى أجهزة الكمبيوتر.					
(ج)	**مخاطر ضعف إجراءات الرقابة the weakness of control procedure risks**					
27	ضعف نظم الرقابة في الجامعة وعدم فعاليته.					
28	اشتراك بعض الموظفين في استخدام نفس كلمات السر					
29	عدم الفصل بين المهام والوظائف المتعلقة بنظم المعلومات والاتصالات.					
30	عدم وجود سياسات وبرامج محددة ومكتوبة لأمن نظم المعلومات والاتصالات.					
31	عدم توفر الحماية الكافية ضد مخاطر فيروسات الكمبيوتر في الجامعة.					
32	عدم التوصيف الدقيق للهيكل الوظيفي والإداري *الذي يحدد المسؤوليات والصلاحيات لكل شخص داخل الجامعة الإسلامية – بغزة.*					
33	لا توجد سياسة واضحة تجبر الموظفين علي تغير الرقم السري كل فترة زمنية					

ت	الفقـرة	بدائـل الإجابـة				
		موافق بشدة	موافق	محايد	معارض	معارض بشدة
(ح)	**السياسات و الإجراءات Policies and procedures**					
34	تقوم إدارة الجامعة بإصدار قرارات إدارية خاصة لتجنب مخاطر أمن المعلومات.					
35	تتعهد الإدارة العليا بالجامعة بتطبيق أمن المعلومات.					
36	تتابع إدارة امن المعلومات في تنفيذ إجراءات الحماية المطلوبة.					
37	تقوم إدارة الجامعة بوضع قواعد خاصة بحماية أمن المعلومات ومعاقبة الموظفين المخلين بهذه القواعد.					
38	تقوم إدارة امن المعلومات بوضع خطة حماية شاملة ومعمقة تشمل إغلاق منافذ الاختراق، والتدقيق في الإجراءات الداخلية والاحتفاظ بنسخة احتياطية من المعلومات يمكن الرجوع إليها عند الضرورة.					
39	تطبق إدارة حماية أمن المعلومات مثل الخصوصية، وتجنب تغيير البيانات غير المصرح به، وتوفر البيانات في الوقت المحدد.					
40	تقوم إدارة امن المعلومات بتحليل المخاطر الخاصة بأمن المعلومات مثل العائد المتوقع مقابل تكاليف الإجراءات المضادة.					
41	تقوم إدارة امن المعلومات باعتماد سياسات خاصة بأمن المعلومات فيما يتعلق باختيار التقنية المناسبة وآلية العمل بها.					

ت	الفقـرة	بدائـل الإجابـة				
		موافق بشدة	موافق	محايد	معارض	معارض بشدة
42	تقوم إدارة امن المعلومات بتركيب طرق الحماية التقنية مثل جدران النار Firewalls ومضادات الفيروسات وغيرها.					
43	تقوم إدارة امن المعلومات بتحديث طرقة الحماية حسب التغيرات الحاصلة في بيئة التكنولوجيا.					
44	تقوم إدارة امن المعلومات بتحليل حوادث الاختراق من خلال التقارير، وتحديد ووصف نوع الاختراق.					
45	تقوم إدارة امن المعلومات بصد الاختراق عند حدوثه وإصلاح الخلل الناتج عنه و عدم تكراره.					
46	تستفيد إدارة الجامعة من خبرة الجامعات العالمية في مجال أمن المعلومات والاتصالات.					
47	هل للطلاب دور في اختراق النظام					
48	هل تكرار الاختراق من جهات محددة					