إقـــــرار

أنا الموقع أدناه مقدم الرسالة التي تحمل العنوان:

The Impact of Information Security Strategic Planning on Information Security Level ،Through the Perspective of Managers and Specialists in Government Institutions in Gaza.

Case Study(Ministry of Communication and Ministry of Interior)

أقر بأن ما اشتملت عليه هذه الرسالة إنما هو نتاج جهدي الخاص، باستثناء ما تمت الإشارة إليه حيثما ورد، وإن هذه الرسالة ككل أو أي جزء منها لم يقدم من قبل لنيل درجة أو لقب علمي أو بحثي لدى أي مؤسسة تعليمية أو بحثية أخرى.

DECLARATION

The work provided in this thesis, unless otherwise referenced, is the researcher's own work, and has not been submitted elsewhere for any other degree or qualification

Student's name: اسم الطالب/ة: مجدولين علي أبو شعير

Signature: التوقيع:

Date: التاريخ: 2016 / 01 / 31

The Islamic University- Gaza
Deanship of Graduates Studies
Faculty of Commerce
Business Administration Department

The Impact of Information Security Strategic Planning on Information Security Level ,Through the Perspective of Managers and Specialists in Government Institutions in Gaza.

Case Study(Ministry of Communication and Ministry of Interior)

أثر التخطيط الاستراتيجي لأمن المعلومات على مستوى أمن المعلومات من وجهة نظر المدراء والمختصين في المؤسسات الحكومية في غزة.

دراسة حالة (وزارة الداخلية ووزارة البريد والاتصالات)

Submitted by:
Majdoleen Ali Abushair

Supervised by
Dr.Akram Ismail Samor

A research submitted in partial fulfillment of the requirement for the Degree of master of business administration

2016

بسم الله الرحمن الرحيم

الجامعة الإسلامية – غزة
The Islamic University - Gaza

الجامعة الإسلامية غزة
The Islamic University - Gaza

مكتب نائب الرئيس للبحث العلمي والدراسات العليا **هاتف داخلي** 1150

الرقم ....ج س غ/35/ Ref

التاريخ 2016/01/16م...... Date

نتيجة الحكم على أطروحة ماجستير

بناءً على موافقة شئون البحث العلمي والدراسات العليا بالجامعة الإسلامية بغزة على تشكيل لجنة الحكم على أطروحة الباحثة/ **مجدولين علي محمد أبو شعير** لنيل درجة الماجستير في **كلية *التجارة*/** قسم **إدارة الأعمال** وموضوعها:

أثر التخطيط الاستراتيجي لأمن المعلومات على مستوى أمن المعلومات من وجهة نظر المدراء والمختصين في المؤسسات الحكومية في غزة. دراسة حالة (وزارة الداخلية و وزارة البريد والاتصالات)

The Impact of Information Security Strategic Planning on Information Security Level ،Through the Perspective of Managers and Specialists in Government Institutions in Gaza.
Case Study (Ministry of Communication and Ministry of Interior)

وبعد المناقشة التي تمت اليوم الاثنين 01 ربيع الآخر1437هـ، الموافق 2016/01/11م الساعة الواحدة ظهراً، اجتمعت لجنة الحكم على الأطروحة والمكونة من:

د. أكرم إسماعيل سمور	**مشرفاً و رئيساً**	....
أ.د. يوسف حسين عاشور	**مناقشاً داخلياً**	....
أ.د. سامي سليم أبو ناصر	**مناقشاً خارجياً**	....

وبعد المداولة أوصت اللجنة بمنح الباحثة درجة الماجستير في **كلية *التجارة*/**قسم <u>إدارة الأعمال</u>.

واللجنة إذ تمنحها هذه الدرجة فإنها توصيها بتقوى الله ولزوم طاعته وأن تسخر علمها في خدمة دينها ووطنها.

والله ولي التوفيق ،،،

شئون البحث العلمي والدراسات العليا
الجامعة الإسلامية غزة
The Islamic University
Research & Graduate Affairs

مساعد نائب الرئيس للبحث العلمي والدراسات العليا

أ.د. عبد الرؤوف علي المناعمة

بسم الله الرحمن الرحيم

[يَا أَيُّهَا الَّذِينَ آَمَنُوا لَا تَخُونُوا اللَّهَ وَالرَّسُولَ
وَتَخُونُوا أَمَانَاتِكُمْ وَأَنْتُمْ تَعْلَمُونَ]

(الأنفال:٢٧)

Abstract

This study aimed to identify" The impact of strategic planning of information security on the level of information security through the perspective of managers and specialists in government institutions in Gaza". The research used the analytical descriptive approach in order to meet research objectives using (SPSS). Study population was (57) employees of staff of the ministry of communication and ministry of interior, those whose their work associated closely to information security and strategic planning, the sample was (50) according to Retched Geger formulation, (50) questionnaires were distributed as a tool to explore the opinions of the study sample, the collected questionnaires were (50), represent response rate (100%).

The findings of the research show that

- Strategic planning of information security impact positively on the level of information security.
- The level of impact of information security strategic planning on the level of information security was approximately (60.73%) Clear weaknesses were found in some fields of strategic planning like: (Implementation of the strategic plan for information security, ccontrol and monitoring of the strategic plan).
- There are no differences among the respondents in their opinions in regard to "the impact of strategic planning of information security on the level of information security through the perspective of managers and specialists in government institutions in Gaza" attributed to their personal information (age, gender, work field, experience, qualification, specialization, training course).

The study concluded several recommendations, the main were as follows:

- Palestinian government are recommended to exert more efforts towards strategic planning for information security.
- Palestinian government are advised to enhance training in fields of information security and strategic planning for it.
- Palestinian government are advised to convert written information security policies to strategic plans.
- Palestinian government are advised to allocate suitable budget for strategic planning of information security.

الملخص

هدفت الدراسة إلى التعرف على أثر التخطيط الاستراتيجي لأمن المعلومات على مستوى أمن المعلومات من وجهة نظر المدراء والمختصين في المؤسسات الحكومية في غزة. استخدمت الباحثة المنهج الوصفي التحليلي لتلبية أهداف البحث واستخدمت لتحليل البيانات برنامج الحزمة الإحصائية (SPSS). تضمن مجتمع الدراسة (57) موظف من موظفي وزارة الاتصالات ووزارة الداخلية ممن يرتبط عملهم ارتباط وثيق بأمن المعلومات والتخطيط الاستراتيجي, وقد اختيرت عينة مقدرة ب(50) موظف حسب معادلة "Retched Geger "وعليه تم توزيع (50) استبان كأداة لاستكشاف اراء عينة الدراسة وتم جمع (50)استبيان اي ما يمثل نسبة (100%).

خلصت الدراسة الى عدة نتائج اهمها:

- يؤثر التخطيط الاستراتيجي ايجابا على مستوى امن المعلومات.
- مستوى تأثير التخطيط الاستراتيجي لأمن المعلومات على مستوى أمن المعلومات في المؤسسات الحكومية كان حوالي (60.73٪). مع وجود ضعف واضح في بعض مجالات التخطيط الاستراتيجي لأمن المعلومات مثل: (تنفيذ الخطة الاستراتيجية لأمن المعلومات, مراقبة ورصد الخطة الاستراتيجية).
- لا يوجد فروق ذات دلالة احصائية عند مستوى دلالة ≤0.05 بين اجابات المبحوثين حول اثر التخطيط الاستراتيجي على مستوى امن المعلومات في المؤسسات الحكومية من وجهة نظر المدراء والمختصين يعزى الى الصفات الشخصية للمبحوثين (العمر , المؤهل العلمي, الجنس, الخبرة, مجال العمل, التخصص, المسمى الوظيفي).

خلصت الدراسة الى مجموعة من التوصيات أهمها:

- ينصح الحكومة الفلسطينية لبذل المزيد من الجهود نحو التخطيط الاستراتيجي لأمن المعلومات.
- ينصح الحكومة الفلسطينية بتعزيز التدريب في مجالات أمن المعلومات والتخطيط الاستراتيجي لذلك.
- ينصح الحكومة الفلسطينية بتحويل سياسات أمن المعلومات الى الخطط الاستراتيجية.
- ينصح الحكومة الفلسطينية إلى تخصيص ميزانية مناسبة للتخطيط الاستراتيجي لأمن المعلومات.

Dedication

I dedicate this work:

To the one who told me what I'm capable of, to a person who planted inside me that science and morality is the most valuable asset. Giving me the support I needed to have my dream.

(My adorable father)

To someone make me realize that I'm worth everything in this world. That I must be treated like a queen, and that I should never settle for less than what I deserve. Her affection, love, prayer make me able to get success and honor..

(My amazing mother)

To those whom without them I couldn't have succeeded..

(My dear brother and my dear sisters)

To all my teachers who guide, inspire motivate and gave me from their knowledge spring, since my childhood, until this moment..

To my friends who they are part of my soul..

Finally, to all the martyrs of Palestine and Syria, especially my soul mate and best friend from childhood to youth: "Hana'a Diab"

"WISHING PEACE SPREAD ALL OVER THE WORLD"

Acknowledgements

I would like to express my gratitude to my supervisor Dr. Akram Samor for guiding and supporting me through the useful comments, remarks and engagement to complete this master thesis. You have set an example of excellence as role model.

I would like to thank my thesis committee members for all of their guidance through this process; your discussion, ideas, and feedback have been absolutely invaluable.

I would like to thank my research advisor, Dr.Kamal El-Masri, Dr.Khaled Dehliz for their constant enthusiasm and encouragement.

I'd like to thank the research technicians, collaborators, and everyone who contributed to this research. I am very grateful to all of you.

I would especially like to thank my amazing family for the love, support, and constant encouragement I have gotten over the years. In particular, I would like to thank my parents and my sisters. You are the salt of the earth, and I undoubtedly could not have done this without you.

List of Contents

List of Tables

List of Figures

List of Abbreviation

CIA	Confidentiality, integrity and availability
IS	Information System
ISI	Information Security indicators
ISP	Information Security Plan
ISMS	Information Security Management System
ISG	Information Security Governance
ISSP	Information Security Strategic plan
ISO	International Organization for Standardization
IEC	International Electro technical Commission
SBP	Strategic Business Plan
SISP	Strategic Information Systems Plan
PDCA	Plan-Do-Check-Act model
SPSS	Statistical Package for the Social Sciences
KPIs	Key Performance Indicators
KPSIs	Key Performance Security Indicators
PRA	Probabilistic Risk Assessment
MOI	Ministry of Interior
IUG	Islamic University Gaza
ISCA	Information Security Culture Assessment
BCP	Business Continuity Plan
SWOT	Strengths, Weaknesses, Opportunities and Threats

CHAPTER ONE

BACKGROUND CONTEXT

- Introduction
- Research problem,
- Research Objectives
- Research hypothesis,
- Research objectives,
- Research importance,

1.1. Introduction

This era is characterized as the age of information technology, where the information is considered as lifeblood asset of organizations. The indicator of success of any organization is how information is managed, controlled and protected from unauthorized use, disclosure, modification, inadvertent user errors, damage, and loss. Add to, organization's ability to provide information in time, particularly during emergencies and times of crisis.

Most organizations need information systems to survive and prosper. Consequently, these organizations need to be serious about securing their information assets. Hence, many important operations emerge to protect information assets, that is on a large extent depends on the cooperative human behavior (Rhee et. al, 2012).

Employees, whether intentionally or through negligence, often due to a lack of knowledge, are the greatest threat to information security. Studies in information security consistently report that a lack of the manager and user awareness is the number one obstacle to achieving a good information security posture. Information security refers to the preservation of Confidentiality, integrity, and Availability (CIA) of information and the systems that use, store, and transmit information. Awareness of information security is the vigilance in understanding various information security threats and in perceiving vulnerability related to these threats. However, an understanding of threats alone seems insufficient to motivate one to take actual actions (Niekerk & Solms, 2010).

Numerous reports published over the last few years indicate that poor security program management is the major underlying problem. A principal challenge many agencies face is in identifying and ranking the information security risks to their operations which is the first step in developing and managing an effective security program. Taking this step helps ensure that organizations identify the most significant risks and determine what actions appropriate to mitigate them (Boltz,1999).

To ensure the workflow and the completion of organization' tasks effectively, managers and decision-makers must take all measures and policies to study the gaps in information systems, and develop the necessary plans to protect the Confidentiality, Integrity, and Availability (CIA) of information and reduce the risk to the fullest extent. With awareness "that there is no absolute protection as long as there is use of the computers" (Laudon & Laudon 2012).

1.2. Research Problem

The information in government institutions was listed at the top of the list of asset, government institutions have a group of employees (engineers and computer programmers and engineer's networks) to manage information security, and they are solving problems in a good technical way. However the information security is an issue no longer handled just by professionals in institutions. Rather, it has become one of the issues that handled by politicians, strategists and decision-makers" (Gheitas,2007)

The literatures confirmed that the information cannot be absolutely protected, but it is possible to raise the level of information security by using flexible Information Security Strategic Plan (ISSP). There are essential aspects, which, if not taken into account in an information security plan, will surely cause the plan to fail, or at least, cause serious flaws in the plan. These aspects can be used as a checklist by management to ensure that a comprehensive plan has been defined and introduced. Because of the importance of these aspects, they will be involved in this study (Solms & Solms,2005).

during the researcher work at one of the government institutions, the Government Computer center organized a Workshop for government institutions at 06/09/2012,the workshop shows the importance of applying information security policy which has been developed by specialists in the Government Computer and according to international standards, engineer Rami - one of the organizers of the workshop- was clarified a number of common staff-mistakes that cause major security problems, and could cost the ministries exorbitant amounts in addition to legal problems, he stressed raising awareness of the information security among employees. In addition to this workshop the researcher has been read number of articles about information security; the most important of them was (Saqallah 2012) article that entitled "Strategic planning for information security." This article cemented the idea in the mind of researcher, which represented in the study the phases of strategic planning for information security and disclose the serious flaws in strategic planning of information security in the government in Gaza. At the end, it determine the impact of ISSP on the level of information security in the governmental institutions in Gaza.

The research problem could be identified as: To what extent the information security strategic planning (ISSP), impact on raising the level of information security in the government institutions in Gaza, through the perspective of Managers and Specialists?

1.3. Research Objectives

- To investigate if concept and the importance of strategic planning for information security is clear to information system managers and specialists in government institutions
- To evaluate the impact of information security strategic planning in raising the level of information security in government institutions in Gaza
- To understand the correlations between strategic planning fields and the level of information security
- To define the priorities should be addressed by the government with regard to information security strategic planning.
- To obtain essential conclusions and recommendations that should enhance the information security strategic planning in the government institutions to raise the level of information security.

1.4. Research Importance

1.4.1. For the Researcher:

- This study considered as a rehearsal to the researcher for the use of scientific research methods, in additional to it fitted her interesting in linking the strategic management with information systems and information security.
- It also opens broad prospects for the researcher.

1.4.2. For The Academic and Researchers:

- This research arises from the lack of such researches in Palestinian government sectors (as far as the researcher knows). The research also could be a reference for future researchers concerned in this topic.
- The research results may encourage researchers to do more studies in this area.

1.4.3. For The Organization:

- The results of this study may help officials of information security and senior management in the government institutions to follow strategic plans for information security systematically and continuously.
- Also the results may encourage them to develop plans and to avoid their weaknesses to protect the institution from significant cost may incur it in case of breaches or problems of information by any way.

1.4.4. For The Community

Usually, the information in the governmental institutions does not consider as competitive assets,so the interest in the information security to be unplanned, therefore the results of this study may encourage government institutions and others sectors that dealing with information as asset to adopt strategic planning for information security and work to solve the information security problems strategically not just technically.

1.5. Research Variables

Depending on (Peláez 2010 ; Wheelen & Hunger 2012 ;Siam 2010;Tayh 2008) the researcher has concluded the study‘s variables.

1.5.1. Dependent variables

- The level of information security.

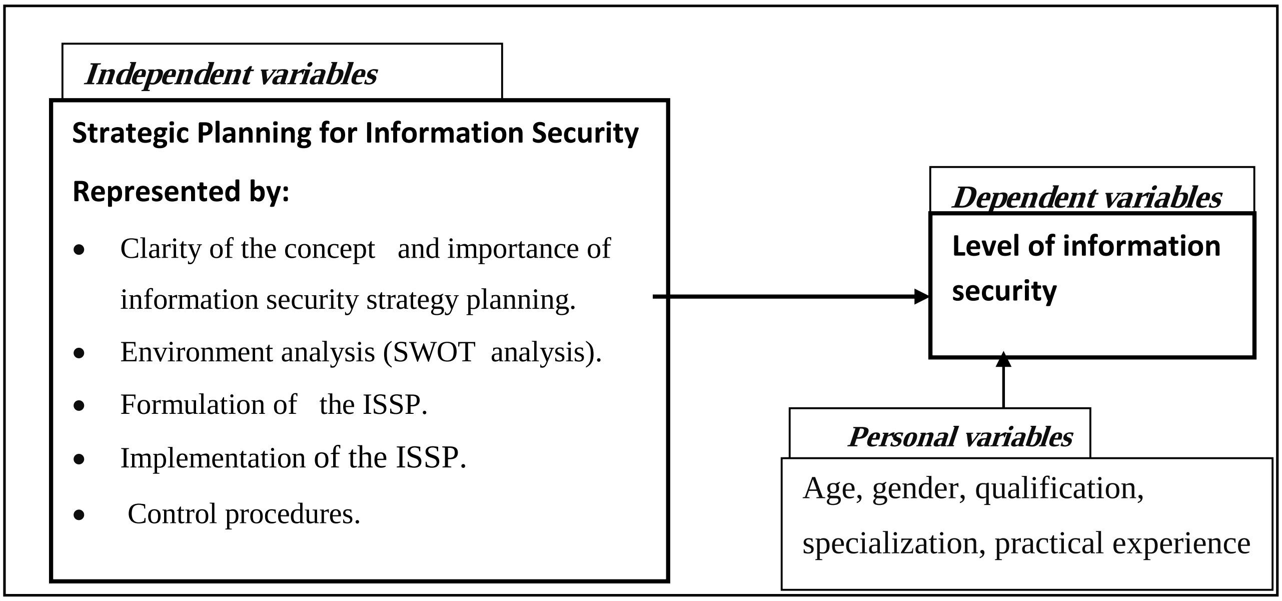
1.5.2. Independent variables

- Strategic Planning for Information Security Represented by:

1. Clarity of the concept and awareness to importance of information security strategy planning.
2. Environment analysis SWOT
3. Formulation of the ISSP.
4. Implementation of the ISSP.
5. Control procedures.

1.5.3. Personal variable

Personal variables (qualification, specialization, practical experience…)


Independent variables
Strategic Planning for Information Security
Represented by:
• Clarity of the concept and importance of information security strategy planning.
• Environment analysis (SWOT analysis).
• Formulation of the ISSP.
• Implementation of the ISSP.
• Control procedures.
Dependent variables
Level of information security
Personal variables
Age, gender, qualification, specialization, practical experience

The figure (1.1) shows the relationship between the variables.

Developed by the researcher (2015) depending on ((Peláez 2010 ; Wheelen & Hunger 2012 ;Siam 2010;Tayh 2008)

1.6. Research Hypotheses

1.6.1. The clarity of the concepts of information security and awareness to importance of information security strategic planning affects positively on the level of information security at the level of statistical significance at $\alpha \leq 0.05$.

1.6.2. Environment analysis affects positively on the level of information security, at the level of statistical significance at $\alpha \leq 0.05$.

1.6.3. The formulation of the strategic plan covering all of the points of SWOT affects positively on the level of information security, at the level of statistical significance at $\alpha \leq 0.05$.

1.6.4. Implementation of the strategic plan affects positively on the level of information security, at the level of statistical significance at $\alpha \leq 0.05$.

1.6.5. Control process on the strategic plan affects positively on the level of information security, at the level of statistical significance at $\alpha \leq 0.05$.

1.6.6. There are statistically significant differences at $\alpha \leq 0.05$ between personal variables (qualification, specialty, years of experience) of managers and specialists of Information systems and the level of information security.

1.7. The Study Scope

- **Place scope**: in the Gaza Strip.
- **Objective scope**: to know the reality of strategic planning for information systems in the government institutions.
- **Institutional scope**: Ministry of Telecommunication and Information Technology**,** and Interior and National Security Ministry
- **Human border**: study applied on managers and specialists of information systems.

CHAPTER TWO
LITERATURE REVIEW

Section one: strategic planning

- Management
- Strategy and strategic
- Strategic management
- Planning
- Strategic planning
- Summary

Section tow: information security

- Introduction
- Information
- Security
- Information security
- Risk management
- Information security strategic planning
- Summary

Section three: government institutions in Gaza

2.1 Introduction

The fast developments that are taking place in life, impose institutions to track the modern scientific methods, in order to be able to adjust and adapts these developments.

The strategic planning relatively is one of the modern topics that the organizations must take care of, to be able to survive in a complex and constantly changing environment. Strategic planning standardizes the processes of goal/objective setting, situation analysis, alternative consideration, implementation and evaluation that enable an organization to attain its goals and objectives (Tapinos et. Al. 2005).

Recently, the information considered the most important asset in the organizations, and its security no longer limited to computer specialists, but has became a strategic goal, and one of the topics that are addressed by politicians, strategists and decision-makers (Gheitas,2007). Accordingly, the formulation, implementation and evaluation of the Strategic Plans for information security to improve the (Confidentiality, Availability, Integrity of information,) are an essential part of the strategic planning cycle of the organization.

The Researcher devoted this chapter to the review of literature that relates to the concept of Strategic planning, information security and Information security strategic planning. The researcher offered those topics through three sections.

- Section I: strategic planning (Basic Concepts)
- Section II: Information Security
- Section III: Governmental Institutions in Gaza

SECTION ONE: STRATEGIC PLANNING

Through searching for the concept of strategic planning in the books and references, the researcher found that most references that dealing with this concept carry “the strategic management” title. This is a logical cause to provide an overview of the concept of strategy and the concept of management, down to Strategy Management and the strategic planning concepts, to clarify the relationship between strategic planning and management, and, at the end, explain strategic planning steps.

2.2.1 Management

The organizations have been around for thousands of years and that management has been practiced for an equivalent period. The development of management theories was characterized by differing beliefs about what managers do and how they should do. (Robbins & Coulter,2009).

The first time the management appeared in the field of industry was in America in the early twentieth century. By scientist Taylor (father of scientific management) "an art of knowing what is to be done and seeing that it is done in the best possible manner", while Henri Fayol (father of modern management) described Management " is to forecast, to plan, to organize, to command, to coordinate and control activities of others"(Galiby & Amiry,2008).

(Robbins & Coulter, 2009) referred to Management as the process of coordinating work activities so that they are completed efficiently and effectively with and through other people. (Schermerhorn,2013) claimed that Management “is a process of planning, organizing, leading, and controlling the use of resources to accomplish performance goals”.

The Researcher summarized all of previous definitions into two elements

- The four-management process.
- Achieve the goals effectively.

2.2.1.1 The Management Process

The management scientists agreed that management made up of four processes Planning, Organizing, Leading and Controlling. (Robbins & Coulter 2009)

1. **Planning: In** management, planning is the process of setting performance objectives and determining what actions should be taken to accomplish them.

2. **Organizing**: Even the best plans will fail without strong implementation. Success begins with organizing, the process of assigning tasks, allocating resources, and coordinating the activities of individuals and groups. When managers organize, they bring people and resources together to put plans into action.

3. **Leading**: is the process of arousing enthusiasm and inspiring efforts to achieve goals.

4. **Controlling**: is the process of measuring performance and taking action to ensure desired results.

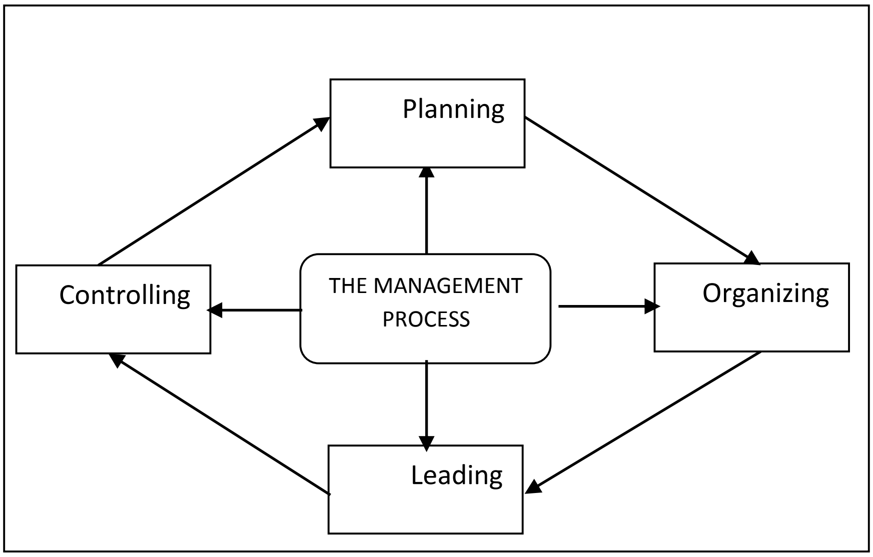


Figure (2.1) shows management processes – developing by Researcher (2015) rely on (Robbins & Coulter 2009)

2.2.2 Strategy and Strategic

*"Without a strategy, an organization is like a ship without a rudder, going around in circles. It's like a tramp; it has no place to go. "**Joel Ross and Michael Kami*** (David, 2011)

2.2.2.1 Strategy

Historically, strategy began in the military field,a that Sun Tzu was the first one who issued a book about Strategy, entitled as (the art of war-in the fourth century BC), the translation was published for the first time in 1910, to guide the military commanders to plan in the fight for victory(Stein 2001).But the first who used the strategy was the ancient Greeks. in 509BC when Athens was at war with the Persians, they created a post (Strategos) means the army commander, and from this word originated the word (Stratêgy) which means "Art of Army leadership or more broadly is the art of leadership(Kordi,2011; Neeuf,2000). Then Napoleon worked to expand this concept as "The science and art face of the enemy through military force" to include economic and political aspects that improve the opportunity of the military component. Then strategic concept moved to the business field, and has become a favorite of use among business organizations especially the modern ones. (Magriby, 1999).

There is no single, universally, accepted definition of strategy, any definition is rooted within the different perspectives adopted by its authors. Strategy, in general, classified under two frameworks, the first one based on the competitive advantage in its essence. (Schermerhorn,2013) saw the Strategy as "a comprehensive plan for achieving competitive advantage ". Porter's opinion Compatible with (Cravens & Piercy, 2006) that strategy " is creation of a unique and valuable position of company, making trade-offs, and forging fit among activities(HBR,2014). Meanwhile, in (Rothaermel,2015) view Strategy "describes the goal directed action at firm intends to take in its quest to gain and sustain competitive advantage".

The second perspective adopted the achievement of the overall objectives of the company through certain activities and opportunities,(this perspective is of interest to the researcher). (Wheelen & Hunger 2012) referred to strategy as " a comprehensive master plan that states how the corporation will achieve its mission and objectives." (Ghoneim, 2006;Yassin,2010; Nickols, 2012; David,2011 ; Kotler2012) view about strategy is" management skills, and means by which long-term objectives will be achieved". (Bateman & Snell, 2010) defined it as " a pattern of actions and resource allocations designed to achieve the organization's goals, Strategy is trying to match the organization's skills and resources to the opportunities found in the external environment. Some time, change or influence the external environment".

Mintzberg concluded all definitions About Strategy and reached a so-called the 5Ps (a **P**lan: a direction, a guide, or a course of action into the future. a **P**loy: a specific maneuver to outwit opponents. a **P**attern: a consistent set of behaviors over time. a **P**osition: a means of locating the organization in place in the environment. and the fifth view is a **P**erspective: an organization's fundamental way of doing things). Note that there are many different interrelations between the 5Ps. (Mintzberg.et.al, 2002)

Researcher adopted that strategy is" a **P**lan designed to achieve the organization's goals using organization's resources and the opportunities found in the external environment".

2.2.2.2 Strategic

The Oxford dictionary defined strategic as "Relating to the identification of long-term or overall aims and interests and the means of achieving them". (Nickolas, 2011) point out: "Clearly, strategic means "of or having to do with strategy." Because strategies can and do exist at various levels of the organization, it is entirely conceivable and appropriate for the corporation to have a strategic plan, for a business unit to have one too, and for a functional unit to have one. Strategic also means "of great significance or importance", intended to address matters of great importance. For those concerned with the enterprise, strategic issues, initiatives, and plans are those that affect the entire enterprise in important ways. Not all strategic issues are long-term, although many are. A short-term crisis can be of strategic significance and should be dealt with accordingly. For our purposes, the strategic means "of great importance."

2.2.3 Strategic Management

Strategic management is the way in which a firm identifies its strategic direction through the use of a more systematic, logical, and rational approach to strategic choice. and aligns its operational processes to its strategy (David. 2011;Mintzberg et.al,1998; Rumelt et.al,1994).In order to get a better understanding of the meaning of the strategy management the researcher presented several definitions:

- Strategic management is the set of decisions and actions used to formulate and execute strategies that will provide a competitively superior fit between the organization and its environment so as to achieve organizational goals (Schermerhorn, 2013)
- It is also a set of managerial decisions and actions that determines the long-run performance of a corporation. Includes: Internal and external environment scanning, Strategy formulation, Strategy implementation and Evaluation and control.(Wheelen & Hunger, 2012).
- It refers to the art and science of formulating, implementing, and evaluating cross-functional decisions that enable an organization to achieve its objectives (David, 2011).

It has been observed that the definitions include three points:

1. Strategic management is Set of managerial decision.
2. It works to achieve the organization's goals and competitive advantage
3. Includes the following stages: environmental scanning, strategy formulation, implementation of the strategy, Evaluation and control.

2.2.3.1 Evolution of Strategic Management

From his extensive work in the field, Bruce Henderson of the Boston Consulting Group concluded that intuitive strategies cannot be continued successfully if (1) the corporation becomes large, (2) the layers of management increase, or (3) the environment changes substantially.As managers attempt to better deal with their changing world, a firm generally evolves through the following four phases of strategic management:

- **Phase 1** - Basic financial planning: Seeking better operational control by trying to meet budgets.
- **Phase 2** - Forecast based planning: Seeking more effective planning for growth by trying to predict the future beyond next year.
- **Phase 3**. Externally oriented planning (strategic planning): Seeking increasing responsiveness to markets and competition by trying to think strategically.
- **Phase 4**. Strategic management: Seeking a competitive advantage and a successful future by managing all resources.

Phase 4 in the evolution of the strategic management includes a consideration of strategy implementation and evaluation and control, in addition to the emphasis on the strategic planning in Phase (3).

General Electric, one of the pioneers of the strategic planning, led the transition from the strategic planning to strategic management during the 1980s. By the 1990s, most corporations around the world had also begun the conversion to strategic management. (Wheelen & Hunger, 2012)

2.2.3.2 Benefits of Strategic Management

(David,2011) stated that Strategic management allows an organization to be more proactive than reactive in shaping its own future; it allows an organization to initiate and influence (rather than just respond to) activities—and thus to exert control over its own destiny.

-**Financially**, Research indicates that organizations using strategic-management concepts are more profitable and successful than those that do not.

-**Nonfinancial Benefits:** add to help the firms to avoid the financial demise, strategic management offers other tangible benefits.

(David,2011; Wheelen & Hunger, 2012) stated that strategic management offers the following benefits:

a. Sharper focus on what is strategically important.
b. It allows for identification, prioritization, and exploitation of opportunities.
c. It provides an objective view of management problems.
d. It represents a framework for improved coordination and control of activities.
e. Improved understanding of a rapidly changing environment and minimizes the effects of changes.
f. It creates a framework for internal communication among personnel.
g. It helps integrate the behavior of individuals into a total effort.
h. It provides a basis for clarifying individual responsibilities.

i. It encourages forward thinking.

j. It gives a degree of discipline and formality to the management of a business.

2.2.4 Planning

In light of technological development at the beginning of the fifties, significant economic and social changes in the United States occurred which led to the change in way of consumption, the concept "long range planning" appeared. (Hamdan & Idris 2009)

The triple verb (plan) in Oxford dictionary defined as **"to design scheme, arrange** beforehand", (Conyers,1985). **Planning** is "an intentional, systematic and prompt effort to achieve a certain goal in a specified period of time and with specific money and effort." (Ghoneim, 2006), while **(**Ganem,2011) represented "planning is the process by which to identify future targets for the market and the development of policies and strategies, and determine the appropriate means to achieve these objectives".(Lyddon,1999; Nickols, 2011) point out that planning involves thinking about the future, identifying and specifying in advance (now) what has to be done or achieved (objectives) and selecting the most suitable means to accomplish these objectives. Successful planning must be accurate and derived from reality and be interactive with all the surrounding circumstances (Nickols, 2011).

According to the perspective of the researcher planning is" the method for determining activities to develop a plan to meets the goals and objectives".

2.2.4.1 The Basic Planning Process.

According to (Bateman & Snell, 2010) the formal planning steps are:

I. Situational analysis summarizes all information relevant to the planning issue under consideration. Thorough situational analysis studies past events, examines current conditions, and attempts to forecast future trends.

II. Alternative Goals and Plans, Based on the situational analysis

III. Goal and Plan Evaluation:(evaluate potential effects of each alternative goal and plan)

IV. Goal and Plan Selection: select the one that is most appropriate and feasible.

V. Implementation of the plan.

VI. Monitor and Control: must continually monitor the actual performance and take corrective action when the plans are implemented improperly.

2.2.4.2 Important Of Planning. (Schermerhorn 2013)

- Planning is the first process of the four functions of management.
- Planning is the process of setting objectives and identifying how to achieve them.

- Planning improves focus and action orientation.
- Planning improves coordination and control.
- Planning improves time management by setting priorities and avoiding time waster.

2.2.4.3 Type of Planning According to Its Impact.

- **Strategic Planning**: Sometimes strategic planning is confused with other planning modalities, each valid in its own right but geared toward a different end result. To put it simply, not every plan is a strategic plan. Strategic Planning is the planning which has great importance for the organization and causing an qualitative impact in it, and practiced by top management where strategic plans are linked with achieving the goals and objectives of the organization.(Hammoud & Lozi,2008), most strategic plans should be reviewed and revamped every three to five years.
- **Tactical planning:** focuses on the implementation of activities in the strategic plans, how to do them, and who will be responsible for completion. time for tactical plans is shorter than the extent of the Strategy plans, as it focuses on Nearby Activities that must be accomplished to achieve the overall strategies of the organization. (Brydson, 2007)
- **Operational Planning** is the process of identifying the specific procedures and processes required at lower levels of the organization. (Bateman &Snell,2010).An operating plan is a coordinated set of tasks for carrying out the goals delineated in a strategic plan. It thus goes into greater details than the strategic plan from which it is derived, spelling out time frames and the roles of individual staff and board members, for example. It also has a shorter horizon than a strategic plan usually one fiscal year.(Mittenthal, 2002**)**

2.2.5 Strategic Planning:

One of the most important management concepts is the concept of strategic planning that well-received and wide-spread in recent years, it is the preparing to face what is expected, also it is a great activity to achieve the objectives that have been developed carefully, as it includes the creation of conducive conditions to absorb and manage the change for those goals.(AlMutawa, 2004)

In the late sixties long-term planning suffered a several criticisms, one of them ,that it ignored the means and tools necessary for implementing the planning process, as a result of that, the strategic planning concept was appeared and replaced the concept of long-term planning, it was a quantum leap, where the strategic planning focused on the critical issues and the challenges in the organizations' life, adding to examine what the organization is, and the environment in which the organization works through(Campo 1980 cited by Hamdan & Idrys 2009).

2.2.5.1 Strategic Planning Definition and Philology.

Strategic planning is the overall planning that facilitates the good management of a process. Strategic planning takes manager outside the day-to-day activities of his organization or project. It provides him with the big picture of what his organization is doing and where it is going. Strategic planning gives manager clarity about what he actually wants to achieve and how to go about achieving it, rather than a plan of action for day-to-day operations. (Shapiro,2003)

Strategic planning has been defined differently by various authors, these definitions have agreed on interest in some aspects, and neglected or minimized of value side or the other aspects; this may be due to the difference in experience and practical experiences of these writers. **Strategic planning** is defined as "the process of developing and maintaining a strategic fit between the organization's goals and capabilities and its changing marketing opportunities." (Kotler & Armstrong, 2012) **Strategic planning According to Bryson** (1995) is a disciplined effort to produce decisions and actions that guide and shape what the organization is, what it does, and why it does it. **Strategic planning** is ongoing; it is "the process of self-examination, the confrontation of difficult choices, and the establishment of priorities" (Pfeiffer et al., 1993).

Strategic planning is more than ensuring your association will remain financially sound and be able to maintain its reserves—it's projecting where your association expects to be in five, ten, or fifteen years—and how your association will get there. It is a systematic planning process involving a number of steps that identify the current status of the association, including its mission, vision for the future, operating values, needs (strengths, weaknesses, opportunities, and threats, goals, prioritized actions and strategies, action plans, and monitoring plans (CAI 2014).

It can be concluded from the above definitions, techniques vary with the particular authors but the substantive issues are essentially the same across authors. These include:

1. setting strategic or enterprise-level financial and non-financial goals and objectives
2. It is an ongoing process.
3. Interview between the internal environment and the external environment

The researcher believed that the essence of strategic planning lied in identifying future opportunities and threats, which can be the basis for decisions at the present time to take advantage of those opportunities, and avoid those threats.

2.2.5.2 Benefit Of Strategic Planning

The goal of strategic planning is to provide a business focus that enhances the firm’s sustainable competitive advantage in key areas. And cuts down management time devoted to chasing serendipitous opportunities. It also **(**Jones 2002;Thomas 2005)

- Work to preparation and development of the administrative leadership for the creative and integrated thinking.
- Takes into account possible changes in the environment to improve effectiveness and impact.
- Provides the necessary foundation for coordination between the different parts of the organization.
- Achieve long-term goals of the organization.
- Strengthen team approaches by defining together a clear focus and direction.
- Enable the best use of the human and financial resources available.
- Strategic planning helps the organization in identifying the causes of problems and how to solve them (Okuma, 2003: P4-6).

2.2.5.3 Constraint of Strategic Planning.

Despite the importance of strategic planning, some firms do not engage in strategic planning, and some firms do strategic planning but receive no support from managers and employees,(David.2011, Hamdan &Idriss 2009, Bimk experts. 2006, Bean 1993.) Stated reasons for poor or no strategic planning as follows:

a. Bad impression among managers of organizations from strategic planning problems.
b. The culture of the organization does not induce participation.
c. The inability of the leaders to strategic planning or the lack of adequate information for strategic planning.
d. Internal conflicts and the absence of control and follow-up.
e. The formulation of the mission does not fit with the specific vision.
f. Carrying out activities that do not respond to the organization's mission and not commensurate with the strategic decisions.
g. The pressure from the environment surrounding the institution.
h. Failing to respond or communicate with target groups
i. Some firms see planning as a waste of time because no marketable product is produced.
j. Some organizations see planning as too expensive in time, money and resource.

k. Lack of trust in management decisions.

2.2.5.4 Relationship Between Strategic Management And Strategic Planning.

Many managers used strategic planning term and strategic management as a single term, this is an error, strategic management is a result of evolution of the concept of strategic planning; strategic planning is part of the strategic management process and an important element of its elements but is not the strategic management. This is because the strategic management also means managing organizational change, management of organizational culture, management of resources and environmental management as well, as it is a strategic management concerned with the present and the future, as it is an inside look to the outside, and look analysis of the present organization of the future perspective, The fundamental difference between strategic planning and strategic management is an area of the gap between planning and strategizing, strategic planning is associated with space and time, that the organization exist, while the strategic management is associated with senior management outlook to the wider world and to the direct and indirect external environment that the organization operates within it's the framework (Yassin,2010)

According to David (2011) the purpose of strategic management is to exploit and create new and different opportunities for tomorrow. Long-range planning, in contrast, tries to optimize for tomorrow the trends of today. The term strategic management is used to refer to strategy formulation, implementation, and evaluation, with *strategic planning* referring only to strategy formulation, because strategic plan is constructed in this stage.

In spite of this, in his text book the term *strategic management* is used synonymously with the term *strategic planning.* This is what has been adopted by the researcher in his research.

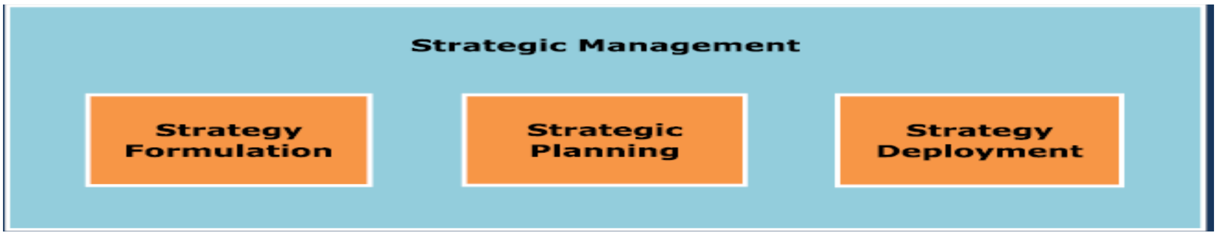


Figure (2.2) display the relation between strategic management and planning (Nickols 2011)

2.2.5.5 Approaches of Preparation Strategic Planning

(Rothaermel,2015) refers that Managers rely on three different approaches to formulate and implement strategy: (1) Top-down Strategic planning, (2) Scenario planning, and (3) Strategy as planned emergence.

1) Top-Down Strategic Planning

This approach typically concentrates strategic intelligence and decision-making responsibilities in the office of the CEO. Top managers adjust the company's vision, mission, and values before formulating corporate, business, and functional strategies. The formulation of strategy is separate from implementation, and thinking about strategy is separate from doing it. Information flows one way only: top-down.

2) Scenario Planning

It is a Strategy planning activity in which managers envision different what-if scenarios to anticipate plausible futures. In a fast-changing environment, there is no way to know where and when the next emergency will arise. Scenario planning asks those "what if" questions. Similar to top-down strategic planning, scenario planning also uses a rational, scientific approach to the strategy process. In addition, in scenario planning managers envision different scenarios, to anticipate plausible futures. How would any of these changes affect a firm, and how should it respond? . The goal is to create strategic plans that are more flexible, and thus more effective, than those created through the more static strategic planning approach.

3) Strategy As Planned Emergence: Bottom-up

Critics of top-down and scenario planning argue that strategic planning is not the same as strategic thinking. In fact, they argue the strategic planning processes are often too regimented and confining. As such, they do not allow for the necessary strategic thinking. Managers doing strategic planning may also fall prey to an illusion of control —that is, the hard numbers in a strategic plan can convey a false sense of security. According to critics of strategic planning, in order to be successful, a strategy should be based on an inspiring vision and not on hard data alone.

In that process, top management does not give any directives to departments, but organizational structure and systems allow bottom-up strategic initiatives to emerge and be evaluated and coordinated by top management, advantages of this Method is that senior management may wish to give freedom of movement to the departments without any limitations Imposed.

2.2.5.6 Models of Strategic Planning and Strategic Management

There are who believe that the lack of agreement about the optimal model for the development of strategies among the problems facing strategic management, and even prove the validity of this view, the researcher displayed a number of strategic planning and management models of some researchers in management.

- **(Wheelen & Hunger,2012)'s model about Strategic management which included:**

1. Environmental scanning
   - External: Opportunities and Threats
   - Internal: Strengths and Weaknesses
2. Strategy formulation
   - Mission
   - Objectives
   - Strategies
   - Policies
3. Strategy implementation
   - Programs
   - Budgets
   - Procedures
4. Evaluation and control
   - Performance

- **(Thompson & et ;2008) model for strategic planning:**

1. Developing a strategic vision
2. Setting objectives
3. Crafting a strategy to achieve the objectives and vision
4. Implementing and executing the strategy
5. Monitoring, developments, evaluating performance, and making corrective adjustments

- **(Rothaermel 2015) model about strategic management: AFI model**

1. Strategy Analysis (A)
   - Strategic leadership and the strategy process(vision, mission, and values)
   - External analysis
   - Internal analysis
   - Competitive advantage
2. Strategy Formulation (F)
   - Business strategy:

- Corporate strategy
- Global strategy

3. Strategy Implementation (I)

- Organizational design: Structure, Culture, and Control
- Corporate governance and business ethics.

2.2.5.7 Stages of Strategic Planning.

Rothaermel (2015) cited strategic management process is a never ending cycle of analysis, formulating, implementing and feedback.

The researcher rely on (Wheelen & Hunger,2012) model to explain the strategic planning process

1. Environmental scanning
2. Strategy formulation
3. Strategy implementation
4. Evaluation and control

2.2.5.7.1 Strategy Analysis(Environmental Scanning)

Environmental scanning is the monitoring, evaluating, and disseminating of information from the external and internal environments to key people within the corporation. Its purpose is to identify strategic factors—those external and internal elements that will determine the future of the corporation. The simplest way to conduct environmental scanning is through SWOT analysis..(Alsaadi 2013) SWOT is an acronym used to describe the particular Strengths, Weaknesses, Opportunities, and Threats that are strategic factors for a specific company.

The external environment consists of variables (Opportunities and Threats) that are outside the organization and not typically within the short-run control of top management. These variables form the context within which the corporation exists. They may be general forces and trends within the natural or societal environments or specific factors that operate within an organization’s specific task environment—often called its industry.

The internal environment of a corporation consists of variables (Strengths and Weaknesses) that are within the organization itself and are not usually within the short-run control of top management. These variables form the context in which work is done. They include the corporation’s structure, culture, and resources. Key strengths form a set of core competencies that the corporation can use to gain competitive advantage (Wheelen & Hunger(2012).

2.2.5.7.2 Strategy Formulation.

This component of strategic management brings in the critical issue of just how the targeted results are to be accomplished. While objectives are the “end product”, the strategy is the “means” of achieving them. The task of formulating the strategy entails taking into account all of the relevant aspects of the organization’s internal and external situation and coming up with a detailed action plan for achieving the targeted short-run and long-run results. Strategy is a blueprint of all the important entrepreneurial, competitive and functional area actions that are to be taken in pursuing organizational objectives and positioning the organization for sustained success.(Nedelea & Paun 2009)

Three integrated phases of crafting a company’s strategy are:

1. Developing a strategic vision of where the company needs to head and what its future focus should be.
2. Setting objectives and using them as yardsticks for measuring the company’s performance and progress.
3. Crafting a strategy to achieve the objectives and move the company along the strategic course has been charted.

STAGE 1: Developing a Strategic Vision, Mission and Value of Company

The first component of the strategic management process is crafting the organization’s mission statement, which provides the framework or context within which strategies are formulated.

- **Strategic vision:** Very early in the strategy-making process, a company’s senior managers must wrestle with the issue of what directional path the company should take. A strategic vision describes management’s aspirations for the future and delineates the company’s strategic course and long-term direction. (Gamble et al.,2013).

An effective vision reduces the risk of rudderless decision-making, pervades the organization with a sense of winning and motivates employees at all levels to aim for the target, while leaving room for individual and team contributions. An inspiring vision helps employees find meaning in their work. Vision statements should be forward-looking and inspiring to provide meaning for employees when pursuing the organization’s ultimate goals. (Rothaerme, 2013), (Thompson et al,2008) in their book put Characteristics of an effectively worded strategic vision as flowing:

1. **Graphic** Paints a picture of the kind of company that management is trying to create and the market position(s) the company is striving to stake out.
2. **Directional** Is forward-looking; describes the strategic course that management has charted and the kinds of product/market/customer/technology changes that will help the company prepare for the future.
3. **Focused** Is specific enough to provide managers with guidance in making decisions and allocating resources.
4. **Flexible** Is not a once-and-for-all-time statement—the directional course that management has charted may have to be adjusted as product/market/ customer/technology circumstances change.
5. **Feasible** Is within the realm of what the company can reasonably expect to achieve in due time.
6. **Desirable** Indicates why the chosen path makes good business sense and is in the long-term interests of stakeholders (especially shareowners, employees, and customers).
7. **Easy to communicate** Is explainable in 5–10 minutes and, ideally, can be reduced to a simple, memorable slogan.

- **Strategic Mission*:*** The defining characteristic of a strategic vision is what it says about the company's future strategic course —"the direction we are headed and our aspirations for the future." In contrast, a mission statement describes the enterprise's current business and purpose **(** Thompson et al,2008), A company should define its business in terms of three dimensions: who is being satisfied, what is being satisfied and how customer needs are being satisfied(Hill & Jones2012)

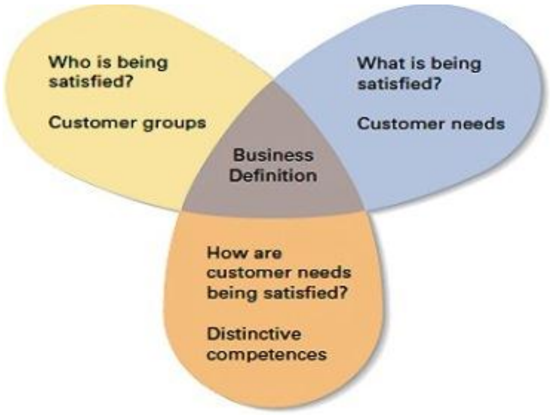


*Figure (2.3) :(*business definition (Hill & Jones 2012)

Is documented in the literature that firms with a formalized mission statement have average return on shareholders' equity and certain financial measures than those firms without a formalized mission, and there is a positive relationship between mission statements and organizational performance. King and Cleland recommend that organizations carefully develop a written mission statement in order to reap the following benefits:

1. To ensure unanimity of purpose within the organization.
2. To provide a basis, or standard, for allocating organizational resources.
3. To establish a general tone or organizational climate.
4. To serve as a focal point for individuals to identify with the organization's purpose and direction, and to deter those who cannot from participating further in the organization's activities.
5. To specify organizational purposes and then to translate these purposes into objectives in such a way that cost, time, and performance parameters can be assessed and controlled (David.2011).

◖ **Company value*:*** The values of a company state how managers and employees should conduct themselves, how they should do business, and what kind of organization they should build to help the company achieve its mission. Insofar as they help drive and shape behavior within a company, values are commonly seen as the bedrock of a company's organizational culture, culture is often seen as an important source of its competitive advantage (Hill& Jones, 2012).

STAGE 2: Setting Strategic Goals and Objectives.

Goals and Objectives, as put forward by (Hill& Jones, 2012)(Gambl et al,2013), are organization's performance targets—the results and outcomes management wants to achieve. They function as yardsticks for measuring how well the organization is doing. The purpose of goals and objectives is to specify with precision what must be done if the company is to attain its mission or vision. Goals are generally more comprehensive or far-reaching than objectives. Framed clearly, they answer the question "What do we want to accomplish?". Well-stated objectives are quantifying able, or measurable, and contain a deadline for achievement.

◖ **Kind of Objective to Set**

Two very distinct types of performance yardsticks are required: financial objectives and strategic objectives. Financial objectives communicate management's targets for financial, strategic objectives relate to target out comes that indicate a company is strengthening its market standing, future business prospects, and competitive vitality. (Hill& Jones, 2012)

Financial and strategic objectives should include both near-term and longer-term performance targets. Short-term (quarterly or annual) objectives and longer term targets (three to five years off), when tradeoffs have to be made between achieving long-run objectives and achieving short run objectives, long-run objectives should take precedence (unless the achievement of one or more short-run performance targets has unique importance).

STAGE 3: Crafting a Strategy and Policies

- **Strategies*:*** Strategies are the means by which long-term objectives will be achieved. That requires top management decisions and large amounts of the firm's resources. Strategies affect an organization's long-term prosperity, typically for at least five years, and thus are future-oriented. Strategies have multifunctional or multidivisional consequences and require consideration of both the external and internal factors facing the firm. For maximum impact, it is advisable to select a combination of strategies for each strategic aim. (Thomas,2005 ;David,2011)

The pioneers of the administration declared that the typical business firm usually considers three types of strategy: corporate, business, and functional.(Smith,2005; Thompson et.al 2008)

1. **Corporate strategy** describes a company's overall direction in terms of its general attitude toward growth and the management of its various businesses and product lines. Corporate strategies typically fit within the three main categories of stability, growth, and retrenchment.
2. **Business strategy** usually occurs at the business unit or product level, and it emphasizes improvement of the competitive position of a corporation's products or services in the specific industry or market segment served by that business unit. Business strategies may fit within the two overall categories, competitive and cooperative strategies.
3. **Functional strategy** Functional strategy is the approach taken by a functional area to achieve corporate and business unit objectives and strategies, it directed at improving the effectiveness of operations.

Business firms use all three types of strategy simultaneously. A hierarchy of strategy is a grouping of strategy types by level in the organization. Hierarchy of strategy is a nesting of one strategy within another so that they complement and support one another. Functional strategies support business strategies, which, in turn, support the corporate strategy (ies).

- **Policies*:*** In addition to strategic and operational plans, organizations also need plans that provide members with day-to-day guidance on such things as attendance, hiring practices, ethical behavior, privacy, trade secrets, and more. This is often provided in the form of organizational policies and procedures.

A policy is a standing plan that communicates broad guidelines for making decisions and taking action in specific circumstances. Policies allow consistency and coordination within and between organizational departments to make sure that employees throughout the firm make decisions and take actions that support the corporation’s mission, objectives, and strategies.

◖ A Strategic Plan

A Strategic Vision + Objectives + Strategy = A Strategic Plan

Developing a strategic vision and mission, setting objectives, and crafting a strategy, together, they constitute a strategic plan for coping with industry and competitive conditions, the expected actions of the industry’s key players, and the challenges and issues that stand as obstacles to the company’s success.(Thompson et.al 2008)

Characteristics of a Successful Strategic Plan

- A living, changing document that is used at meeting regularly to insure the organization is on the defined strategic path.
- A realistic and comprehensive assessment of SWOT analysis.
- A clear and comprehensive grasp of external opportunities and challenges.
- An empowered planning committee.
- Sharing responsibility by board and staff members.
- Learning from best practices.
- Clear priorities and implementation.
- Patience
- Commitment (NMF 2011)

2.2.5.7.3 Strategy Implementation

No matter how brilliant the formulated strategy, the organization will not benefit if it is not skillfully executed. Strategy execution requires that all aspects of the organization be in congruence with the strategy and that every individual’s efforts be coordinated toward accomplishing strategic goals. Each company manager has to think through the answer to “What has to be done in my area to execute my piece of the strategic plan, and what actions should I take to get the process under way?” (Gamble et.al 2013)

The implementation stage is an operations-oriented phase that managers must make things happen. Arguably it is the most demanding and time-consuming part of the strategic management process. It requires preparing a strategic plan that sets out annual objectives,;

Installing policies and procedures that facilitate strategy implementation, establishes an effective organizational structure capable of carrying out the strategic plan, fixes a budget, develops a viable information system and generally devices a work plan for job execution. It also involves motivating employees, creating a supportive culture, allocating resources and Linking the motivation and reward structure directly to achieving the targeted results.(Thompson et al, 2008).

Good strategy execution requires diligent pursuit of operating excellence. It is a job for a company's whole management team. Success hinges on the skills and cooperation of operating managers who can push for needed changes in their organizational units and consistently deliver good results. (Gamble et al 2013)

(Wheelen & Hunger 2012) elucidate that strategy implementation include the development of programs, budgets and procedures.

Programs: A program is a statement of the activities or steps needed to accomplish a single use plan. The purpose of program is to make a strategy action oriented.

Budgets: A budget is a statement of corporation's program in monitory terms. After programs are developed, the budget process begins. Planning a budget is the last real check a corporation has on the feasibility of its selected strategy. An ideal strategy might found to be completely impractical only after specific implementation programs are coasted in detail.

Procedures: Procedures are system of sequential steps or techniques that describe in detail how a particular task or job is to be done

2.2.5.7.4 Evaluation And Control of Strategy

Strategies evolve regularly in response to changes in an organization's internal situation and external environment. What qualifies as a high-performance strategy today is sooner or later rendered stale by events unfolding both inside and outside the company. The task of "strategizing" can never therefore be a one-time exercise, strategic planning is an ongoing process; it never ends, Once a strategy has been implemented, the corporate activities and performance results must be monitored to determine the extent to which strategic goals and objectives are actually being achieved. This information and knowledge pass back up to the Managers at all corporate levels through feedback loops to take timely corrective action. or to stimulate the entire process to become the input for the next round of strategy formulation and implementation. (Hill& Jones 2012; Wheelen & Hunger 2012; Thompson et.al 2008)

Performance is the end result of activities. It includes the actual outcomes of the strategic management process. The practice of strategic management is justified in terms of its ability to improve an organization's performance, typically measured in terms of profits and return on investment. For evaluation and control to be effective, managers must obtain clear, prompt, and unbiased information from the people below them in the corporation's hierarchy. Using this information, managers compare what is actually happening with what was originally planned in the formulation stage.

2.2.6 Summary

The researcher summarized this section as the flowing:

- Strategic Management is the basis of organizations' success in complex environment, flexibility strategic planning depends on the environment scanning and involving people in all levels of management, in order to formulate a good vision, goals and continuously improve work methods, procedures and evaluation techniques to take advantage of environmental changes .
- There are a lot of obstacles may prevent the implementation of the strategic planning but successful management ultimately is working to overcome these obstacles.
- The administration should choose the best model of planning models which fits with its resources.
- Strategic Planning does not stop when implementing the plan, but it's core process is to monitor activities and evaluate the performance to ensure that the objectives have been achieved and manage any deficiency.

SECTION 2: INFORMATION SECURITY

2.3 Introduction

In this era, the information becomes increasingly valuable, and the organization with the best information on which to base management decisions will be the likeliest to win and prosper (Finne, 2000 in Gupta & Sharman, 2012). It is therefore essential to secure information properly against all possible information security threats (from inside as well as outside the organization). (Kritzinger & Smith,2005; Gupta& Sharman, 2012).information security has crossed the IT department frontiers and reached business and support areas because companies discovered that Information is one of its most valuable asset, and the company that has the right information in the right time will succeed against its competitors.

2.3.1 Information

The word information is used commonly in our day-to-day working. In management information system (MIS), information has a precise meaning and it has different meaning from data. The information has a value in decision making while data does not have. Information brings clarity and creates an intelligent human response in the mind (Pesante 2008).

Information is a set of data transformed in such a way that it:

- Improves representation of an entity
- Updates the level of knowledge.
- Has a surprise value.
- Reduces uncertainty.
- Aids in decision making (Menguzzato & Renau,1991 Quoting (Alcamí & Carañana, 2012))

ISO 17799 defines information as an asset that may exist in many forms and has value to an organization.

2.3.1.1 Information Characters

(Bagad,2008; Alcamí & Carañana, 2012) referred that good information must be characterized by the following:

- **Accuracy**: Information must be sufficiently accurate for managers' purposes.
- **Punctuality**: Good information is that which is delivered just when it is needed.
- **Conciseness**: where the user receive brief information, It will save time and can be accessed to brevity across relevant data summarization.
- **Comprehensiveness**: that the information contains all the data needed to make a decision-.Accuracy: the percentage of correct information to the total number of processor data during the period Specific.
- **Relevance** is a decisive quality. Relevant information is what increases knowledge and reduces uncertainty surrounding the problem under consideration.
- **Clarity**: means that the information must be made clear and legible, and therefore the Provider of information must be aware of the level of knowledge of the recipient and his culture and what he loves.
- **Validity:** The validity of the information relates to the purpose of the information. In other words, it is the answer to the question-dose the information meet the purpose of decision making for which it is being collected?

2.3.1.2 Classification of the Information

Organizations classify information in order to the appropriate levels of protection for these resources. Because resources are limited, it will be necessary to prioritize and identify what really needs protection. One of the reasons to classify information is to ensure that scarce resources are employed where they will do the best.

All information is seems equal, but not all of them has the same value. From all of the information found within an enterprise, approximately only 10% of it is actually considered as competitive advantage, trade secret, or personal information. The biggest portion of organization information is information that is typically accessed by most or all employees to do their assigned tasks. The remaining information has been made available to the public through authorized channels. Information resources that are classified as public would include annual stockholders' reports, press releases, and other authorized public announcements.(Peltier,2014)

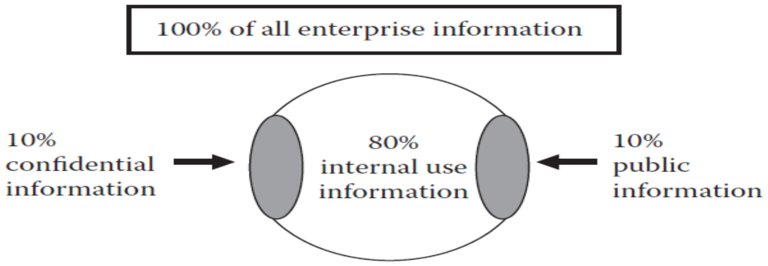

100% of all enterprise information
10% confidential information
80% internal use information
10% public information

Figure (2.4) Information classification breakdown (Peltier 2014)

The information can be classified under the terms of its application (Piccol,G.,2013).

- **Planning information**

Certain standards, norms and specifications are used in the planning of any activity. Hence, such information is called the planning information. The time standards, the operational standards, the design standards are the examples of the planning Information.

- **Control information**

Reporting the status of an activity through a feedback mechanism is called the control information. When such information shows a deviation from the goal or the objective, it will induce a decision or an action leading to control.

- **Knowledge information**

A collection of information through the library reports and the research studies to build up acknowledge base as an information source for decision making is known as Knowledge information. Such a collection is not directly connected to decision making, but the need of knowledge is perceived as a power or strength of the organization.

The information can also be classified based on its usage. When the information is used by everybody in the organization, it is called the **organization information**. When the information has a multiple use and application, it is called the **database information**. When the information is used in the operations of a business it is called the functional or the operational information.

2.3.2 Security

Security is essential for humans; it is located at the second level in the Maslow pyramid. At the past the traditional concept of security was "derivative of power".

The goal of Barry Buzan in his book ***People, States and Fear***, was to offer a "broader framework of security" incorporating concepts that were not previously considered to be part of the security puzzle such as regional security, or the societal and environmental sectors of security "Security is taken to be about the pursuit of freedom from threat and the ability of states and societies to maintain their independent identity and their functional integrity against forces of change, which they see as hostile. The bottom line of security is survival" (Stone,2009).In management science security as one of six activities of management identified by Henry Fayol is "Protection of property and person". Security is often used interchangeably in the literature to mean computer security, Internet security, network security and information security (Goh, 2003).

2.3.3 Information Security

2.3.3.1 Definition of Information Security:

- Computers are becoming a basic component of everyday operations, and organizations depend on them. A failure in computer system could have a critical impact on the organization, so the potential vulnerabilities in a computer system that may cause a wide range of threats to Information (Shim et al, 2000). So information Security is used to protect information in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities (Ladan et al., 2006).
- Compounding the definitional problems of information security is that it is viewed essentially as being synonymous with computer security although their meanings differ.

Researcher displayed some definitions of the computer security concept and information security concept to bring out the deference between the two concepts.

- **Computer security**
  - **Is defined by Stallings(2008) as"** The protection afforded to an automated information system in order to attain the applicable objectives of preserving the CIA of information system resources (includes hardware, software, firmware, information/data, and telecommunications
  - **And by (Howard, 1997)** " security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks"
  - **As for (Webopedia, 2002) it** "refers to techniques for ensuring that data stored in a computer cannot be read or compromised*"*.
- **Information Security**

- Is defined as "policies, procedures and technical standards that are used to prevent unintentional access, theft or destruction of records" (Sultan,2009).
- "The result of any system of policies and/or procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute. (SANS Institute, 1998)
- Information Security involves the use of physical and logical data access controls to ensure the proper use of data and to prevent unauthorized or accidental modification, destruction, disclosure, loss or access to automated or manual records and files as well as loss, damage or misuse of information assets (Peltier, 2014).
- Information Security is also "a well-informed sense of assurance that information risks and controls is in balance" (Anderson, 2003).
- The Committee on National Security Systems (CNSS) defines information Security as" the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information".

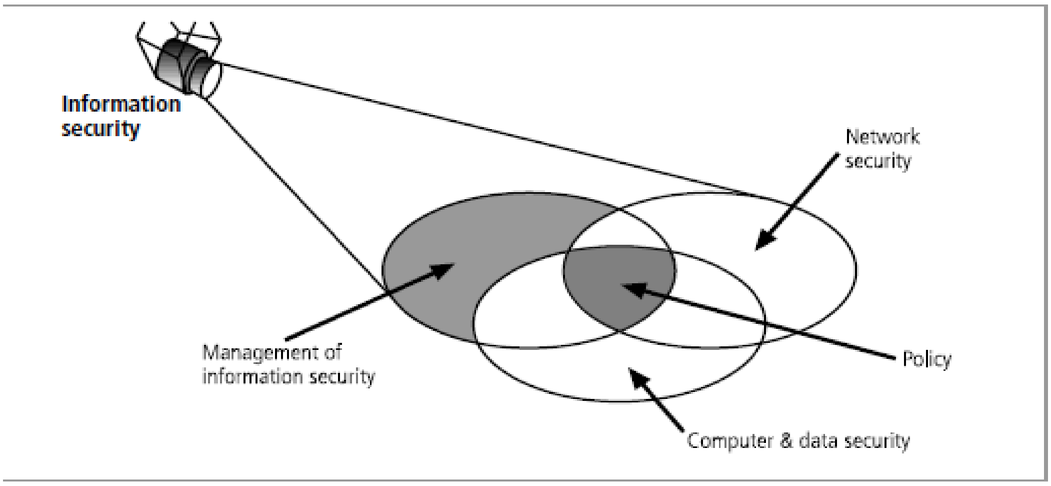


Figure (2.5): Components of information security(Whitman & Mattord 2012.p9)

From the definitions above, key points stand out are:

1. Information is the most important asset that needs protection .
2. Talking about security implies talking about entities of a technological nature.
3. Information security is different from computer security in that it is a goal, whereas computer security is the mean toward that goal: information security.
4. Information security main purpose is to protect the valuable resources and assets of an organization, such resources could be in the form of information, hardware, and software.
5. Information security includes the broad areas of information security management, computer and data security, and network security.

2.3.3.2 Evaluation Of Information Security

(Zidane, 2010) determined: During the sixties of the last century the concept of security was about limiting access data, or external manipulation of the devices ,at that time the computer security concept appeared, which means protecting computers and databases. The seventies witnessed transition to the concept of data security to control access to the data, in addition to measures to protect computers from disasters, and adopt plans retrieved data, and store extra copies away from the computers. In 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

2.3.3.3 Important of Information Security

(Whitman &Mattord,2012) pointed that information security performs four important functions for an organization:

1. Protecting the organization's ability to function
2. Enabling safe operating of applications running on the organization's IT systems
3. Protecting the data in which the organization collects and uses
4. Safeguarding the organization's technological assets

1. Protecting the organization's ability to function

Both general management and IT management are responsible for implementing information security that protects the organization's ability to function. Although many business and government managers abstain from handling information security because they perceive it to be a technically complex task, implementing information security has more to do with management than with technology.

2. Enabling the Safe Operation of Applications

Today's organizations are under immense pressure to acquire and operate integrated, efficient, and capable applications. A modern organization needs to create an environment that safe guards these applications. Once an organization's infrastructure is in place, management must continue to oversee it, and not relegate its management to the IT department.

3. Protecting Data that Organizations Collect and Use

Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers. Even when transactions are not online, protecting data in motion and data at rest are both critical aspects of information security. The value of data motivates attackers to steal, sabotage, or corrupt it. An effective information security program implemented by management protects the integrity and value of the organization's data.

4. Safeguarding Technology Assets in Organizations

To perform effectively, organizations must employ secure infrastructure services appropriate to the size and scope of the enterprise. For example, organizational growth could lead to the need for Public Key Infrastructure (PKI), an integrated system of software, encryption methodologies, and legal agreements that can be used to support the entire information infrastructure.

2.3.3.4 Information Security Objectives

The goal of information security must be consistent with the objectives of the organization, to achieve a set of requirements. (Debi,2008) which are Confidentiality, Integrity, and Availability (CIA) of information. According to (Peitier, 2001; Hansche et.al 2004 ;Stamp,2006;Pesante, 2008; stalling 2008) The three objectives (CIA) are stated as:

1) **Confidentiality:**

When information is read or copied by someone not authorized to do so, the result is known as loss of confidentiality. "Confidentiality is the protection of information within systems so that unauthorized (people, resources and processes) cannot access that information". 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 handling such data.

2) Integrity

Integrity by ISO-17799 is defined as “Safeguarding the accuracy and completeness of information and processing methods”. Integrity is particularly important for critical safety and financial data used for activities. Integrity can be examined from three perspectives: (Stewart et.al, 2004)

- Unauthorized subjects should be prevented from making modifications.
- Authorized subjects should be prevented from making unauthorized modifications.
- Objects should be internally and externally consistent so that their data is a correct and true reflection of the real world and any relationship with any child, peer, or parent object is valid, consistent, and verifiable

3) Availability

Information can be erased or become inaccessible, resulting in loss of availability. Availability: assures that systems work promptly and service is not denied to authorize users whenever needed. Availability is often the most important attribute in service-oriented businesses that depend on information.

To achieve the objectives organizations need to use a set of standards relating to the people who use that information are: “AAA” Authentication, Authorization, and Auditing. Pesante (2008); (Hansche et al 2004); (Shaw, et.. al, 2009 in Altoom 2013)

a. Authentication and Authorization(Access control)

Authentication goes hand in hand with authorization, and usually they are explained under the term "Access control”. Access control is about the relationships between subjects and objects. The transfer of information from an object to a subject is called access. A foundational principle of access control is to deny access by default if access is not granted specifically to a subject. Stamp (2006) pointed out that the term access control refers to issues concerning access of system resources. Under this broad definition, there are two primary parts to access control, namely, authentication and authorization. Authentication deals with the problem of determining whether a user (or other entity) should be allowed access to a particular system or resource. However, an authenticated user is generally not given carte blanche access to all system resources. it must somehow restrict the actions of authenticated users. This is the field of authorization.

These two aspects of access control can be summarized as

•Authentication: Who goes there?

• Authorization: Are you allowed to do that?

➢ **Authentication Methods**

- **Something you know “PASWORD”:** It is any string of characters that you have memorized and can reproduce on a keyboard when prompted; Passwords are used to verify that the user of an ID is the owner of the ID. The ID-password combination is unique to each user and therefore provides a means of holding users accountable for their activity on the system.” (Tipton, 2004)
- **Something you are “BIOMETRICS”: is method** of authentication or, in Schneider's immortal words “you are your key”. There are many different types of biometrics, including such traditional examples as fingerprints and handwritten signatures. Stamp (2006).Fingerprint is considered the most popular biometric characteristic for identification and authentication. (Fried, 2004)
- **Something you have:** It is a physical device that you are in possession of and must have on your person at the time of authentication, Smartcards can be used for authentication based on “something you have.”(Stewart et al, 2004)

b. Auditing

The final plank in the AAA framework is auditing, which measures the resources a user consumes during access. Auditing covers a wide variety of different activities, logging, monitoring, examining alerts, analysis, and even intrusion detection.(Stewart et al, 2004)

- **Logging:** Logging is the activity of recording information about events or occurrences to a log file or database.

- **Monitoring:** Monitoring is the activity of manually or programmatically reviewing logged information looking for something specific.
- **Alarm triggers:** Alarm triggers are notifications sent to administrators when a specific event occurs.
- **Log analysis:** Log analysis is a more detailed and systematic form of monitoring in which the logged information is analyzed in detail for trends and patterns as well as abnormal, unauthorized, illegal, and policy-violating activities.
- **Intrusion detection:** Intrusion detection is a specific form of monitoring both recorded information and real-time events to detect unwanted system access (Stewart et al, 2004).

2.3.3.5 Element of Information Security

The various means of protection designed to provide protection in the following position, which represents at the same time the elements of information security system: (Altoom, 2013; Stewart et al, 2004; Bayuk, 2014)

1. **Privacy:** 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**: it mean making sure that the information is not disclosed nor seen by individuals not authorized to do so.
5. **Authentication:** it means making sure of the identity of the person who is trying to use the information, 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 which 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**: Non-repudiation ensures that the subject of an activity or event cannot deny that the event to occurred. Non-repudiation prevents a subject from claiming not to have sent a message, not to have performed an action, or not to have been the cause of an event. It is made possible through identity, authentication, authorization, accountability, and auditing. Non-repudiation can be established using digital certificates, session identifiers, transaction logs, and numerous other transactional and access control mechanisms.

2.3.3.6 Threats of Information security

"Know the enemy, and know yourself, and in a hundred battles you will never be in peril"
Sun Tzu

Knowing the enemy faced by information security is a vital component to shaping an information security defense posture. In the context of information security, a threat is an object, person, or other entity that presents an ongoing danger to an asset (Whitman & Mottord,2012)

2.3.3.6.1 Security Threat Source

The greatest threat to information security lies not beyond the security perimeter (hackers, malware, etc.), but rather with the careless or malicious actions of internal users such as employees and other trusted constituents with easy access to organizational information resources (Willison and Warkentin, 2013; Pfleeger and Caputo, 2012; Posey et al.,2011; Warkentin and Willison, 2009; Capelli et al., 2006).

(Peltier et al 2005) has confirmed that the information is under threat not only from outside the organization but the biggest threats may be from inside, Institute (CSI) in San Francisco estimates that between 60 and 80 percent of network misuse comes from inside the enterprise.

- **Internal threats**

Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network. A threat can be internal to the organization as the result of employee action or failure of an organization process.

- **External threats**

External threats can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. The most obvious external threats to computer systems and the resident data are natural disasters: hurricanes, fires, floods and earthquakes. External attacks occur through connected networks (wired and wireless), physical intrusion, or a partner network. (Ngoma, 2012)

2.3.3.6.2 Threat Agents

(Jouini et al 2014) referred that the threat agent is the actor that imposes the threat to the system. We identified three classes for our specific classification: humans, natural disasters and technological threats. The proposed classification covers the full set of potential agents since we include humans, chemical and physical reaction on human-made objects (technological),and, natural for all those agents on which humans do not have any influence.

- **Human Threats**

This class includes threats caused by human actions such as insiders or hackers which cause harm or risk in systems.

- **Environmental factors**

Environmental threats are threats caused by non-human agent. It comes, first, from natural disaster threats like earthquakes, flood, fire, lightning, wind or water and, also, due to animals and wildlife which cause severe damage to information systems like floods, lightning, Tidal Waves (like Tsunami) and fire. Indeed, this class includes other threats such as riots, wars, and terrorist attacks.

- **Technological Threats**

Technological threats are caused by physical and chemical processes on material. Physical processes include the use of physical means to gain entry into restricted areas such as building, compound room, or any other designated area like theft or damage of hardware and software. However, chemical processes include hardware and software technologies. It, also, includes indirect system support equipment like power supplies. (Ngoma, 2012)

2.3.3.6.3 Threats Classification

Management must be informed of the different threats facing the organization. A firm can build more effective security strategies by identifying and ranking the severity of potential threats to its IS efforts. (Whitman & Mattord, 2012) denote that Threats or dangers facing an organization’s people, information, and systems fall into the following categories:

- Compromises to intellectual property
- Deliberate software attacks
- Deviations in quality of service
- Espionage or trespass
- Forces of nature
- Human error or failure
- Information extortion
- Missing, inadequate, or incomplete organizational policy or planning
- Missing, inadequate, or incomplete controls
- Sabotage or vandalism
- Theft
- Technical hardware failures or errors
- Technical software failures or errors
- Technological obsolescence

2.3.3.6.3.1 Compromises to intellectual property

Intellectual property is defined as “the ownership of ideas and control over the tangible or virtual representation of those ideas. Use of another person’s intellectual property may or may not involve royalty payments or permission, but should always include proper credit to the source.”

Attacks on Intellectual Property (IP) come in a variety of forms including :(Safe Net, 2013)

- Software piracy
- Reverse engineering & theft of trade secrets
- Code tampering

Each of these poses a serious threat to software revenue and future innovation for software publishers and intelligent device manufacturers

- **Software piracy:** Many individuals and organizations do not purchase software as mandated by the owner’s license agreements. Because most software is licensed to a particular purchaser, its use is restricted to a single user or to a designated user in an organization. If the user copies the program to another computer without securing another license or transferring the license, he or she has violated the copyright.

- **Reverse engineering & theft of trade secrets:** Reverse engineering, "is the process of extracting knowledge or design information from anything man-made and re-producing it or reproducing anything based on the extracted information".
- **Tampering:** Tampering occurs when someone gains access to your software code and makes a change to how the product functions. It's important to realize that tampering can be intentional and malicious, or accidental and with good intent.

2.3.3.6.3.2 Deliberate Software Attacks

Deliberate software attacks occur when an individual or group designs and deploys software to attack a system. Most of this software is referred to as malicious code or malicious software, or sometimes malware. These software components or programs are designed to damage, destroy, or deny service to the target systems. Some of the more common instances of malicious code are viruses and worms, Trojan horses, logic bombs, and back doors. (Whitman & Mattord, 2012)

- **Virus:** A computer virus consists of segments of code that perform malicious actions. As with biological viruses, computer viruses have two main functions propagation and destruction. The code attaches itself to an existing program and takes control of that program's access to the targeted computer. The virus-controlled target program then carries out the virus's plan by replicating itself into additional targeted systems. computer viruses are passed from machine to machine via physical media, e-mail, or other. (Stewart et. al, 2004)
- **Worms:** are interesting types of malicious code that greatly resemble viruses, with one major distinction. Worms are self-replicating. They remain resident in memory and exploit one or more networking vulnerabilities to spread from system to system under their own power. (Stewart et.al, 2004).
- **Trojan horse:** "A Trojan horse is a code fragment that hides inside a program and performs a disguised function" (Hansche et.al, 2004).Trojan horses are frequently disguised as helpful, interesting, or necessary pieces of software, such as readme.exe files often included with shareware or freeware packages. (Whitman & Mattord, 2012)
- **Logic bombs**: are malicious code objects that lie dormant until events occur that satisfy one or more logical conditions. At that time, they spring into action, delivering their

malicious payload to unsuspecting computer users. They are often planted by disgruntled employees or other individuals who want to harm an organization.(Stewart et.al, 2004).

- **Trap Doors - Back Doors:** A virus or worm can have a payload that installs a back door or trap door component in a system. Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource through a back door. Sometimes these entries are left behind by system designers or maintenance staff, and thus are called trap doors. A trap door is hard to detect, because very often the programmer who puts it in place also makes the access exempt from the usual audit logging features of the system. (Whitman &Mattord,2010)

2.3.3.6.3.3 Deviations in quality of service

The denial-of-service (or DoS) Attack is an attempt to make a machine or network resource unavailable to its intended users. Attacker sends large number of connection or information requests to a target

- Target system cannot handle successfully along with other, legitimate service requests
- May result in system crash or inability to perform ordinary functions
- Mail bombing: also a DoS; attacker routes large quantities of e-mail to target
- Deviations in quality of service can result from incidents such as a backhoe taking out a fiber-optic link for an ISP. (Whitman &Mattord,2012, Handley et al.2006)

2.3.3.6.3.4 Espionage or trespass

Espionage or trespass is a well-known and broad category of electronic and human activities that can breach the confidentiality of information. When an unauthorized individual gains access to the information an organization is trying to protect, that act is categorized as espionage or trespass. Attackers can use many different methods to access the information stored in an information system. Some information gathering techniques are quite legal, for example, using a web browser to perform market research. These legal techniques are called, collectively, competitive intelligence. Shoulder surfing occurs anywhere a person accesses confidential information. (Ngoma, 2012)

2.3.3.6.3.5 Human error or failure

This category includes acts performed without intent or malicious purpose by an authorized user. When people use information systems, mistakes happen. Inexperience, improper training, and the incorrect assumptions are just a few things that can cause these misadventures.

Risky practices in which employees routinely engage, that are directly related to information security: Ponemon (2012)

- Connecting computers to the internet through an insecure wireless network.
- Not deleting information on their computer when no longer necessary.
- Sharing passwords with others.
- Reusing the same password and username on different websites.
- Leaving computers unattended when outside the workplace (or data storage in unprotected areas for example desktop).
- Losing a USB drive possibly containing confidential data and not immediately notifying their organization.
- Working on a laptop when traveling and not using a privacy screen.
- Carrying unnecessary sensitive information on a laptop when traveling.
- Using personally owned mobile devices that connect to their organization’s network.
- Entry of erroneous data, aaccidental data deletion or modification.

Regardless of the cause, even innocuous mistakes can produce extensive damage. Employees are the threat agents closest to the organizational data. Their mistakes represent a serious threat to the CIA of data.

However, if someone damages or destroys data on purpose, the act belongs to a different threat category.

2.3.3.6.3.6 Forces of Nature

Forces of nature, force majeure, or acts of God can present some of the most dangerous threats, because they usually occur with very little warning and are beyond the control of people. These threats, which include events such as fires, floods, earthquakes, and lightning as well as volcanic eruptions and insect infestations, can disrupt not only the lives of individuals but also the storage, transmission, and use of information. (Ngoma, 2012)

2.3.3.6.3.7 Information extortion

Information extortion occurs when an attacker or trusted insider steals information from a computer system and demands compensation for its return or for an agreement not to disclose it. Extortion is common in credit card number theft. (Whitman & Mattord,2012)

2.3.3.6.3.8 Missing, Inadequate, or Incomplete Organizational Policy or Planning

Missing, inadequate or incomplete organizational policy or planning makes an organization vulnerable to loss, damage, or disclosure of information assets when other threats lead to attacks. information security is, at its core, a management function. The organization's executive leadership is responsible for strategic planning for security as well as for IT and business functions—a task known as governance. (Whitman &Mattord,2012)

2.3.3.6.3.9 Missing, Inadequate, or Incomplete Controls

Missing, inadequate, or incomplete controls—that is, security safeguards and information asset protection controls that are missing, misconfigured, antiquated, or poorly designed or managed—make an organization more likely to suffer losses when other threats lead to attacks. For example, if a small organization installs its first network using small office/home office (SOHO) equipment and fails to upgrade its network equipment as it becomes larger, the increased traffic can affect performance and cause information loss. Routine security audits to assess the current levels of protection help to ensure the continuous protection of organization's assets. (Ponemon, 2012)

2.3.3.6.3.10 Sabotage or Vandalism

This category of threat involves the deliberate sabotage of a computer system or business, or acts of vandalism to either destroy an asset or damage the image of an organization. These acts can range from petty vandalism by employees to organized sabotage against an organization. Although not necessarily financially devastating, attacks on the image of an organization are serious. Vandalism to a web site can erode consumer confidence, thus diminishing an organization's sales and net worth, as well as its reputation. There are innumerable reports of hackers accessing systems and damaging or destroying critical data. Compared to web site defacement, vandalism within a network is more malicious in intent and less public.. (Whitman &Mattord,2012)

2.3.3.6.3.11 Theft

The threat of theft—the illegal taking of another's property, which can be physical, electronic, or intellectual- is a constant. The value of information is diminished when it is copied without the owner's knowledge. Physical theft can be controlled quite easily by means of a wide variety of measures, Electronic theft, however, is a more complex problem to manage and control. If thieves are clever and cover their tracks carefully, no one may ever know of the crime until it is far too late.

Social engineering: using social skills to convince people to reveal access credentials or other valuable information to attacker. (Das, 2014)

2.3.3.6.3.12 Technical Hardware Failures or Errors

Technical hardware failures or errors occur when a manufacturer distributes equipment containing a known or unknown flaw.

2.3.3.6.3.13 Technical Software Failures or Errors

Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved. Sometimes, combinations of certain software and hardware reveal new bugs. These failures range from bugs to untested failure conditions. Sometimes these bugs are not errors, but rather purposeful shortcuts left by programmers for benign or malign reasons. Software bugs are so commonplace that entire Web sites are dedicated to documenting them. (Whitman &Mattord,2011).

2.3.3.6.3.14 Technological Obsolescence(Das,2014)

Outdated infrastructure can lead to unreliable and untrustworthy systems. Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity from attacks. Management's strategic planning should always include an analysis of the technology currently in use. Ideally, proper planning by management should prevent technology from becoming obsolete, but when obsolescence is manifest, management must take immediate action. IT professionals play a large role in the identification of probable obsolescence.

2.3.3.7 Information Security Management

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.* "Sun *Tzu.

Information security Management in an organization requires the organization to identify its information assets and implementing of policies, standards procedures and guidelines that insure the information availability, integrity and confidentiality (Hansche et.al, 2004). (Eloff & Eloff, 2003) stated that the process of ISMS consists of two phases, namely, planning and then implementing management practices, procedures and processes for establishing and maintaining information security. According to (Posthumus & Solms, 2004), the ISMS process consists of:

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

ISO/IEC 27001:2005 adopts a process approach for implementing ISMS in the organization.

This process approach consists of the Plan-Do-Check-Act (PDCA) model:

1. **Plan (establishing the ISMS):**Establish the policy, the ISMS objectives, processes and procedures related to risk management and the improvement of 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

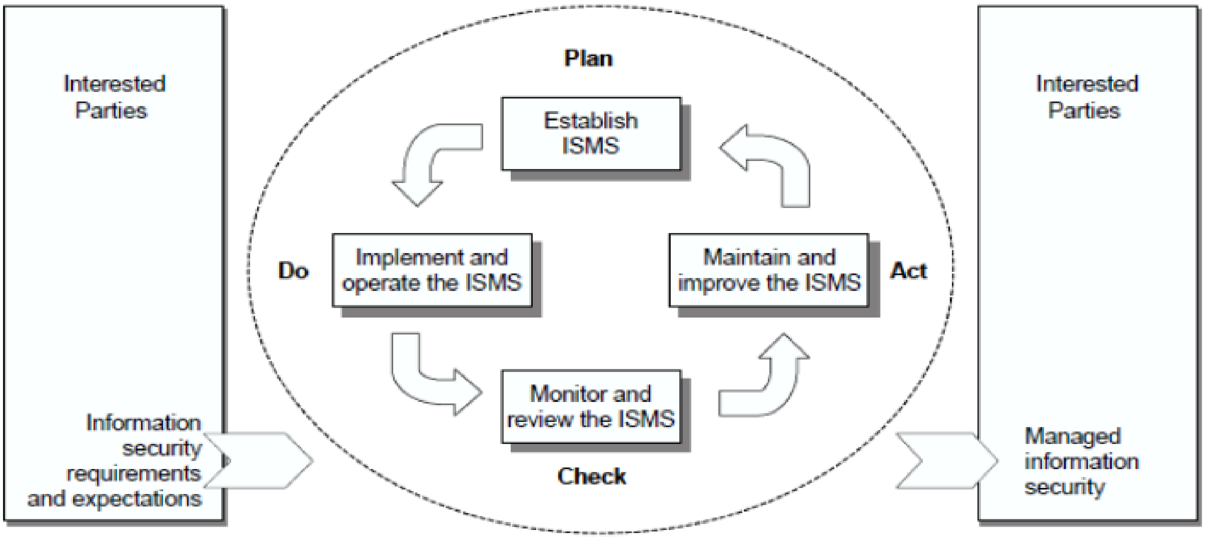

Interested Parties
Information security requirements and expectations
Plan
Establish ISMS
Do
Implement and operate the ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Interested Parties
Managed information security

Figure (2.6) (PDCA) model - ISO/IEC 27001

From the perspective of the researcher, these four operations represent a strategic planning process o

2.3.3.8 The Governance of Information Security

Security governance is "the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly (Gregory,2009).

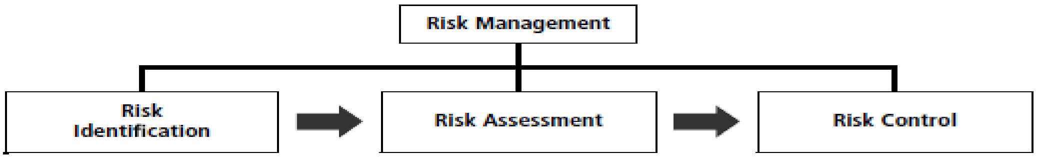
The governance of Information Security is a strategic planning responsibility whose importance has grown over recent years. Unfortunately, information security is all too often regarded as a technical issue when it is, in fact, a management issue .Information Security objectives must be addressed at the highest levels of an organization's management team in order to be effective and sustainable. When security programs are designed and managed as a technical specialty in the IT department, they are less likely to be effective. A broader view of information security encompasses all of an organization's information assets, including the knowledge managed by those IT assets.

2.3.3.9 Risk Management

This term characterizes the overall process. The first phase, risk assessment, includes identification of the assets at risk and their value, risks that threaten a loss of that value, risk-reducing measures, and the budgetary impact of implementing decisions related to the acceptance, mitigation, or transfer of risk.

The second phase of risk management includes the process of assigning priority to, budgeting, implementing, and maintaining appropriate (CRC 2004)

Risk management involves three major undertakings: risk identification, risk assessment, and risk control.



figure(2.7):Risk management (Whitman& Mattord,2012)

2.3.3.9.1 Risk Identification

Risk identification is the examination and documentation of the security posture of an organization’s information technology and the risks it faces. (Whitman& Mattord,2012)

The required from information security professionals to know their organizations’ information assets and identifies the risks facing each asset and taking steps to reduce this risk to an acceptable level. The assets that related to information are:

i. **People**: employee (end users and IS specialists, system analyst, programmers, data administrators etc.) and Nonemployees (include contractors and consultants etc.).
ii. **Hardware**: (Physical computer equipment and associate device, machines and media).
iii. **Software**: Software components are assigned to one of three categories: applications, operating systems, or security components
iv. **Procedures**: Procedures fall into two categories: IT and business standard procedures, and IT and business sensitive procedures.).
v. **Data**: (data and knowledge bases)
vi. **Networks**: communications media and network support. (Whitman & Mottord,2012)

2.3.3.9.2 Risk Assessment

In information security area the risk assessment or risk analysis is defined as “analysis of the potential threats against an asset and the likelihood that they will materialize.”

- **Probabilistic risk assessment (PRA)** (or probabilistic safety assessment/ analysis) is a systematic and comprehensive methodology to evaluate risks associated with a complex engineered technological entity. Risk in a PRA is defined as a feasible detrimental outcome of an activity or action. In a PRA, risk is characterized by two quantities:

1. The magnitude (severity) of the possible adverse consequence(s), and
2. The likelihood (probability) of occurrence of each consequence.(Shing&Shing 2010)

2.3.3.9.3 Risk Control Strategies

Whitman& Mattord (2012) indicate that Organizations have five choices to choose from in order to deal with the risk if they assessed that they could be exposure to such risk

1 Defend

The defend control strategy attempts to prevent the exploitation of the vulnerability. This is the preferred approach and is accomplished by means of countering threats, removing vulnerabilities from assets, limiting access to assets, and adding protective safeguards. There are three common methods used to define:

- Application of policy
- Education and training
- Application of technology.

2 Transfer

The transfer control strategy attempts to shift risk to other assets, other processes, or other organizations. This can be accomplished by rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing insurance, or implementing service contracts with providers.

▪ Advantages outsourcing:
- Outsource company focuses their energy and resource on their expertise.
- Allows parent company to concentrate on the business they know. Example Kodak.

▪ Disadvantages:
- Cost tends to be high for these services, and they require very detailed legal contracts.

3 Mitigate

The mitigate control strategy attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation. This approach requires the creation of three types of plans: the incident response plan, the disaster recovery plan, and the business continuity plan. Each of these plans depends on the ability to detect and respond to an attack as quickly as possible and relies on the quality of the other plans. Mitigation begins with the early detection that an attack is in progress and a quick, efficient, and effective response.

4 Acceptance

In contrast to other control, acceptance is a method of doing nothing to protect vulnerabilities and accept the outcome of its exploitation. To use this control the following must be taken into account.

-Determined the level of risk.

-Assessed the probability of attack.

-Estimated the potential damage that could occur from attacks.

-Performed a thorough cost benefit analysis.

-Take in account the feasibility of other controls.

-Decide if particular functions /assets/data do not justify the cost of protection.

5 Terminate

The terminate control strategy directs the organization to avoid those business activities that introduce uncontrollable risks. By terminating the questionable activity, the organization reduces the risk exposure.

Evaluation, Assessment, and Maintenance of Risk Controls

The selection and implementation of a control strategy is not the end of a process; the strategy, and its accompanying controls, must be monitored and reevaluated on an ongoing basis to determine their effectiveness and to calculate more accurately the estimated residual risk. This cycle is a process that continues for as long as the organization continues to function.

2.3.3.10 Information Security Strategic Planning

Strategic planning sets out the long-term direction to be taken by the whole organization and by each of its component parts. Strategic planning should guide organizational efforts and focus resources toward specific, clearly defined goals. After an organization develops a general strategy, it generates an overall strategic plan by extending that general strategy into strategic plans for major divisions.

The purpose of an information security strategy is to provide management with the necessary information to make informed decisions about investment in security. The strategic plan links the security function with the business direction. The strategy must present a business case that describes key business benefits and outcomes related to security, with recommended strategies for achieving those outcomes (Wentworth, 2003)

An information security strategic plan begins with vision, objectives, policy, standards, and practices.

2.3.3.10.1 Security vision

The vision is the picture of the future environment, showing how people, process and technology, with work together to overcome constraints and threats, and meet all security objectives. (Wentworth, 2003)

2.3.3.10.2 Security objectives

Security objectives are the subset of the business objectives that can be achieved by application of the security functions.

Strategic security must achieved List of objectives

a. To reduce security events
b. To provide security infrastructure that reduces development costs.
c. To reduce operational costs (reduce insurance costs by reducing the risk profile of the organization
d. To protect assets by performing risk assessment
e. To reduce fraud.
f. To reduce legal penalties.
g. To provide consulting to reduce risks.

2.3.3.10.3 Security Policy

Information security policy was identified by (Bowen et.al, 2006) " A collection of directives, rules, and practices that prescribes how an organization manages, protects, and distributes the information ".

The goal of the security policy is to translate, clarify and communicate management's position on security as defined in high-level security principles. The security policies act as a bridge between these management objectives and specific security requirements (Weiseand Martin, 2001).Policy should be short, constituted of series of clear and specific points, not more than one side of paper, because the shorter document is the more read one by employees.

Security policy should contain:

- Information security roles and responsibilities;
- Security controls baseline and rules of exceeding the baseline; and
- Rules of users' behavior and minimum consequences for noncompliance (Bowen& et al, 2006).

2.3.3.10.3.1 Types of Policies

The three types of policies that described by (Hare, 2004) are:

- **Regulatory**: Regulatory policies are security policies that the organization is required to implement, because it consists of some regulations or/and legal requirements imposed by the government bodies to organize some certain of professions like medicine and law.
- **Advisory**: Advisory policies are not mandated, but it's strongly suggested to be followed in some events such as job warning and termination.
- **Informative**: Informative Policies are not mandate too, its purpose is to inform the individuals with some information, and no consequences on individuals if they are not follow or apply it.

2.3.3.10.3.2 Contents of the Policy

The following issues should be addressed by the policy.

- **Access Control Standards:** Every user should be granted the only needed permissions that allow him/her to access the information systems and services that make him/her capable of doing his/her duties.
  - Accountability: It is important that users are held accountable for all actions carried out under their user IDs.
  - Audit Trails: The actions carried out by users must be recorded and logged.
- **Backups:** The backup of the databases, users' files and software should be done in a regular basis, and the backup media should be kept in a secure place. The backup media will be used in case of failure or loss of data, and restore the corrupted or lost files and applications.
- **Business Continuity Plans:** Business Continuity Plan (BCP) should be developed, updated, and tested. Such plan will be used for all critical information systems and services to minimize the restore time of the business in case of failure.
- **Physical Security:** There should be a policy to protect the information facilities from physical side, such policy should make sure those information systems, removal storage media, electrical and communication services are well protected against unauthorized access as far as possible, these protection controls should be consistent with a cost-efficient operation.
- **Viruses: I**t's very necessary for the organization to have an antivirus installed on all computers, but this not means that the staff members are not responsible in this manner, they should make sure that files should be checked before being loaded to the network, and they should report any detected viruses to the IT department in the organization.

- **Noncompliance:** The policy should also contain the actions that the organization may take if the staff member not compliance with the security policy, and the staff members should be noticed and know such actions.
- **Legislation:** The security practitioner should be conversant with the legislations that relevant to the aspect of information security, in order not to violate these legislations and put his/her organization in a critical situation (Harold F. Tipton & Micki Krause CRC 2004).

2.3.3.10.3.3 Policy versus Procedures

Shorten (2004) argues that the policy defines and states what should be done, but procedures tell how that thing should be done. For example, if the policy says, "All users must have a password", the procedure would tell more information about that password, in terms of its length, its lifetime, level of complexity.. etc.

2.3.3.10.4 Staff Awareness

The authors of the report argue that one of the most effective counter measures against human factor threats to information security are security awareness, training and education. If you put a good policy, but your staff does not understand it, the policy will be useless. So, the staff members should be educated, and feeling that the policy will protect them.(Hare, 2004). The motivation for security awareness is increasing the compliance of the employees to detect attacks in an earlier phase.

2.3.3.10.5 Evaluation of Information Security.

- **Directive Controls:** Usually called administrative controls; their purpose is to advice the employees on how their behavior should be when they interact with organization’s information systems. These directives always presented as policies or related documents.
- **Preventive Controls:** Preventive controls are mechanisms to prevent undesirable actions to be occurred. Some examples of these controls are guards, mantraps, backups, UPS, separation of duties, and user registration.
- **Detective Controls:** They are about using practices, processes, and tools that detect and react to security violations. Some examples of these controls are audit trails, intrusion detection, logs, and violation reports.
- **Corrective Controls**: These controls contain a physical, administrative, and technical measures designed to react to any detection of an incident in order to reduce or eliminate its occurrence again.

- **Recovery Controls:** Once a violation has occurred, recovery controls are necessary to restore the system or operation to its normal operating state. The recovery control could be restoring a lost or corrupted file from the backup (Hansche et.al, 2004, P: 341–342).

2.3.3.10.6 Auditing

Auditing is a methodical examination or review of an environment to ensure compliance with regulations and to detect abnormalities, unauthorized occurrences, or outright crimes. Secure IT environments rely heavily on auditing. Auditing covers a wide variety of different activities, logging, monitoring, examining alerts, analysis, and even intrusion detection.

2.3.3.10.6.1 Key Performance Indicators

Key Performance Indicators (KPIs) are quantifiable variables which can measure the performance of an organization, evaluate the success of specific activities and support decision making processes. The usage of KPI in the field of Information Assurance is at its early stage. Defining KPIs for the Security Assurance processes is difficult because of the complexity of regulations, certifications, technical and organizational issues, and budget constraints. Hence it is a complex task to quantify clear Security Assurance objectives and performance in terms of KPIs.

- **Key Performance Security Indicators (**KPSIs) can measure the maturity level of the information security processes (detection and detection-related processes.

-The first purpose of KPSIs is to assess the organization's overall maturity level of security event detection and response posture.

- The second purpose of KPSIs is to enable an organization to assess the actual detection levels of security events as summarized in (ISI 001-1) information security indicators and to evaluate the results of the measurements

2.3.4 Summary

The current era is the era of information and is not the era of industries, the information in the business world is the assets which upon it the decisions are made. hence the companies must classify their information according to their importance to the decisions, Information may be exposed to many threats, some of them from outside the company and some from inside, the internal threats are the most dangerous, companies work to protect sensitive information, by all means, to ensure the three main things is called a security triangle (Confidential, Integration and Availability).

The threat agent is the actor that imposes a threat to the system. Three classes of information threat agent are classified (humans, natural disasters and technological threats).

The process of ISMS consists of two phases, namely, planning and then implementing management practices, procedures and processes for establishing and maintaining Information Security. This phases translate into approach issued by ISO/IEC 27001. The process of this approach consists of the Plan- Do- Check- Act (PDCA) model

Important part of ISMS is Risk management which involves three major undertakings: risk identification, risk assessment, and risk control.

Strategic planning of Information Security as any strategic planning begins with vision, objectives, policy, standards, and practices.

SECTION 3: Government Institutions In Gaza

2.4.1 The Ministry of Interior (MOI)

The Ministry of Interior (MOI) was established to maintain security and discipline in the state of Palestine, and to protect the lives and property of Palestinian citizens in the Gaza strip.

2.4.1.1 Information Systems and Computer' General Department

Information systems and Computer' General Department is one of the actors departments in Interior Ministry, and specializes in providing integrated computerized solutions that actively contribute to finding solutions to many problems, and provide a suitable working environment through linking all the different departments by an integrated network, as well as finding appropriate alternatives, develop work in the ministry, facilitate administrative processes and procedures and provide technical support and maintenance of the ministry network and computer accessories and office equipment and devices. Information Systems and Computer' General Department strives to determine the goals and objectives that serve the public vision and strategic objectives of the ministry.

2.4.1.2 Planning and development unit

It is one of the support units that associated with the Interior Minister, its tasks supporting all the departments and units of the Ministry in the specific items related to planning, policies and projects, development and operations monitoring and evaluation and coordination of international aid.

2.4.2 Ministry of Telecom & Information Technology

2.4.2.1 IT sector

Information technology is a key driver for the development of all science, and is a big supporter of all life activities, and play an important role in advancing the development and knowledge in various fields towards new Prospects. The ministry attaches great importance to this sector by working to provide all means for the success of e-government project and promote the electronic transformation of institutions, government departments and enhance the knowledge of digital in Palestinian society.

2.4.2.2 Government Computer General Directorate

The aims of the Government Computer General Directorate is planning, supervision and implementation of all the items of infrastructural IT.

The General Directorate of Government Computers is a major source of technical information and it is advisory body in the field of information technology and communication, where it is offering its services to all Palestinian National Authority institutions. Design, implement and manage the Palestinian government network that links all of the Palestinian National Authority institutions to each other and with the global information Internet network using the latest technology and ensure confidentiality and security for the flow of data and information across national and international network.

2.4.2.3 General Directorate for Informatics

General Directorate of Information operates to develop of the electronic services, software and database using modern techniques, which would contribute to improve the government performance and raise the level of productivity and transparency of government work. Add to provide technical consultancy in the field of information technology for all government institutions.

2.4.3 General policy of Information Ssecurity In Ministries and Government Institutions

Ministry of telecommunications & Information Technology issued document for information security policies to be applied in government institutions, this document have included on eight areas.

1. **Administrative responsibilities.**
   a. General Directorate and departments
   b. Eexternal actors
   c. Crisis Management
2. **Physical security.**
   a. Environment
   b. Security equipment
   c. Controlling physical access
3. **Access control security.**
   a. Data access control.
   b. Personal check.

c. Privacy.

d. Identification

e. User privileges management

f. Network access.

g. Documenting events.

4. Information Security.

a. Data Privacy

b. Backup

5. Applications security

a. Development and maintenance of applications

b. Management and control of settings

6. Communication and networks security.

a. Network Protection

b. Internet Security

c. protection against computer viruses and malicious code

d. Wireless network security

7. Evaluate and audit the security risks

a. Security risk assessment

b. Security audit

8. Management of Security Event

a. Respond to security incidents

CHAPTER THREE

PERVIOUS STUDIES

- **Introduction**
- **Studies about information security**
  - Local studies
  - Arab and foreign studies
- **Studies relate information security with strategic planning**
  - Local studies
  - Arab and foreign studies

3.1 Introduction

This chapter deals with previous studies that associated with this study, and which from it the researcher derived variables and methodology of this study, the studies are divided into two main groups, the first group is related to information security, and the second group is linked to strategic planning and its relationship to the information security

3.2 Studies about Information Security

3.2.1 Local Studies:

1. **Altoom study (2013)**

The research study titled “Information Security and Communications Management in light of Networks Technology" aimed to manage information and communication security in light of network technology at the (IUG), through Determine the impacts of the input, output data, policies and procedures, and lack experience risks on the security of information and communications in IUG. The analytical descriptive approach was used and the comprehensive survey to introduce the research data in order to meet research objectives using the Statistical Package for the Social Sciences (SPSS). Questionnaires were distributed as a tool in survey the opinions of the research population, the response rate (78%). The study found that statistical significant relationship between the risks on the surrounding technology and the level of system security associated with natural disasters, fire, and Israeli attacks. The system can be penetrated from outside. And the staffs have no experience in the field of updated security programs, policies and procedures. 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.

2. **Eldanaf study (2013)**

The study titled "The reality of management information systems security in the technical colleges in the Gaza Strip and ways of developing” aimed to identify actual situation of information systems security, detecting threats and verification of the effectiveness of methods used for information security. Then determine ways to develop information security management in technical colleges in the Gaza Strip. The questionnaire and interviews were used as tools. The questionnaire analyzed with the SPSS. The study sample was consisted of 123 employees representing all the college’s IT centers engineers and the users of Information Systems in the technical colleges (of which 97 was retrieved). The study found there are differences between the Technical Colleges in applying the information security management due to the age, training levels, staff experience years, rate of security budget. But all technical colleges haven’t any written information security policy, and only some college’s higher management know about it. The study recommended the following: 1) Establishing and developing Information security policy in the technical colleges. 2) Increase the financial budget of information security processes. 3) Increase the capabilities of employees in security fields through training.

3. Tayh study (2008)

The study titled "Effectiveness of Information Security Management at the Palestinian Information Technology Companies" aimed: to identify the extent of the effectiveness of information security management in Palestinian Information Technology companies (Jerusalem, West-bank, and Gaza). Questionnaire and interviews were the tools of study. The questionnaires analyzed with the SPSS. The study sample consisted of 74 Companies of IT (of which 74 was retrieved).The descriptive analytical quantitative technique was used in this research because it is suitable and widely used in analyzing such this topic. The findings of the research showed that all domains except the organizational security were affecting the effectiveness of information security management in Palestinian Information Technology companies. Moreover, there are no differences between the information technology companies in applying the information security management due to the company history in IT field, operating systems, staff qualifications, staff experience years, company main working field, and yearly security budget.

4. Hassan study (2013)

The study titled “Information Security Management for Strategic and Effective Implementation of E-Management in the Governmental Institutions in Gaza" aimed to identify the impact of information security management on the effectiveness of applying e-management in the governmental organizations in Gaza. The research used the analytical descriptive approach and the comprehensive survey to collect the study data in order to meet research objectives (158) questionnaires were distributed as a tool to explore the opinions of the study population, response rate (91.14%). Ten fields of information security management were investigated at (8) governmental organizations along with the effectiveness of applying e-management. The study found that the effectiveness rate of information security management in the governmental oganizations in Gaza was (65.30%). The effectiveness rate of applying e-management was (74.5%). Also found clear weaknesses in some fields include: personnel security, organizational security, compliance to legal requirements and asset classification and control. The study recommended Government is advised to exert more efforts towards the weak information security fields.

3.2.2 Arabic and foreign Studies

5. Veiga & Martins study (2014)

The paper titled "Improving the information security culture through monitoring and implementation actions illustrated through a case study " The aim was to assessed the information security culture in organizations such as the behavior of employees is in compliance with information security and related information processing policies and regulatory requirements, by focusing on developmental areas, of which awareness and training programs. An information security culture assessment (ISCA) system has been developed for this purpose. In this paper discuss a case study of an international financial institution (ISCA), which was conducted at four intervals over a period of eight years, across twelve countries (Australia, Botswana, Guernsey, Jersey, Hong Kong, Ireland, Mauritius ,Namibia ,South Africa, Switzerland, United Kingdom, United States). Comparative and multivariate analyses were conducted to establish whether the information security culture improved from one assessment to the next based on the developmental actions implemented.

The result of study refer that: The information security culture improved from one assessment to the next, with the most positive results in the fourth assessment.This research illustrates that information security training and awareness is a significant factor in positively influencing an information security culture and improve information security level.

6. Abu kmail (2011)

The study titled "The development of internal controls to protect information prepared electronically" aimed to study "Development of internal control for protect the electronic prepared data, and determine the risks created by the use of electronic systems the Palestinian banks.The questionnaire was designed for this purpose. The descriptive analytical method was used and the needed statistical analysis was conducted to test the research hypotheses.The study found: the banks have a Limited number of observers interns, and the most important risks facing the internal control systems in electronic systems that more than one employee used the same password and allow workers to transfer programs files out of the system after working hours to perform certain tasks. There was strict procedure of control in the process of entry and operation and extraction of data and information in the electronic systems.

7. Kazemi et.al(2011)

The study titled "Evaluation Of Information Security Management System Success Factors: Case study of Municipal Organizations" aimed to identify the priority of key success factors in implementing information security management system in Iranian Municipal Organization with the view of experts. The questionnaire was used as a tool to collect data, Questionnaire was distributed to 35 from the study sample the response rate was 100%.The results were analyzed with SPSS software. The study found that factors associated with high levels of the organization (top management and policy) are in the first priorities, and then factors related to staff are in the second priority (training, motivation). Finally, there are factors relating to compliance with security standards and consultants outside the organization. The study was recommended that a research should be done about the causes of low importance of using the services of the information security external advisors.

3.3 Studies Relate to Information Security WITH STRATEGIC PLANNING

3.3.1 Local Studies

8. Dirawi (2014)

The study titled “The relationship of MIS strategic planning with information security in the Palestinian universities in the Gaza Strip.” aimed to examine the relationship between strategic planning of management information systems represented by (vision and mission of MIS, goal setting, environmental analysis, setting priorities, and resource estimate) and information security in the Palestinian universities in the Gaza Strip. The analytical descriptive approach was used and the comprehensive survey to collect the study data in order to meet research objectives using the Statistical Package for the Social Sciences (SPSS). (82) Questionnaires were distributed as a tool to explore the opinions of the study population, the collected questionnaires were (82), represent response rate (100%). The study found that: there is a medium positive correlation between strategic planning of management information systems represented by (vision and mission of MIS, goal setting, environmental analysis, setting priorities, and resource estimate) and information security in the Palestinian universities in the Gaza Strip. And there are significant differences in the responses of the study sample due to the variable name of the university in all domains of the study In favor of Al-Quds Open University.

3.3.2 Arabic and Foreign Studies

9. Hall et.al study (2011)

The study titled "Impacts of organizational capabilities in Information Security" The George Washington University “aimed to examine the relationship between information security strategy and organization performance, with organizational capabilities as important factors influencing successful implementation of information security strategy and organization performance. A questionnaire was used to collect the study data. A questionnaire was mailed to 1,600 respondents residing within the USA and the District of Columbia. The targeted sample population consists of Certified Information System Security Professionals (CISSPs).The study found that evidence suggests the organizational capabilities, encompassing the ability to develop high-quality situational awareness of the current and future threat environment, the ability to possess appropriate means, and the ability to orchestrate the means to respond to information security threats, are positively associated with effective implementation of information security strategy, which in turn positively affects organization performance. However, there was no significant relationship between decision making and information security strategy implementation success. The study recommended: Business leaders should focus on organizational capabilities that provide high valued contributions to the accomplishment of information security strategy goals and organizational objectives, enabling their businesses to achieve market-leading performance and thus competitive advantage.

10. Scanlan (2011):

The study titled” Assessing the alignment of information security, strategic business, and strategic information system planning: A department of defense perspective”. The purpose of this research was to ascertain if alignment existed in the relationship between the Strategic Business Plan (SBP), Strategic Information Systems Plan (SISP) and the Information Security Plan (ISP). A survey was designed to analyze a public organization (the United States Marine Corps) to determine if this alignment is present. A vertical, cross-sectional sample from a Department of Defense organization was surveyed (n = 149). The data were analyzed using the Statistical Package for the Social Sciences (SPSS). The results from this study indicated that information security is present at the strategic planning level. Information security planning should not be thought of as second hand or a part of the SISP. The ISP is a separate planning consideration.

11. Al Sahli (2011)

The study titled ”The Role of Strategic planning requirements in Diminishing Disasters Harms” aimed to determine the role of strategic planning requirements in diminishing disasters harms. The survey analytical methodology was used, Questionnaire was designed to collect data, questionnaire were distributed on (280) officers working in Civil Defense public directorate in Eastern Region The study concluded that: There is high understanding level of strategic planning aspects by Civil Defense officers in Eastern Region for facing disasters. There is deficiency in financial abilities required to apply disasters facing strategies, absence of technologies required to carry out protection and contaminated strategies, facing strategies, control strategies, and rare in qualified manpower required to prepare protection and contaminated strategies, facing strategies, control strategies. The study recommended: 1) Increasing financial abilities required to support Civil Defense in preparing developed strategies to face disasters. 2) Providing advanced training programs in strategic planning field to the Civil Defense staff members, developing communication systems among organization participated in disasters protection.

12. Al-Awadi & Saidan (2010)

The paper titled “Justifying the need for a data security management plan for the UAE" attempted to investigate the need to develop a UAE data security strategy and a detailed framework that can ensure the safety of data and can cope with all types of disasters expected in the country. A questionnaire has been designed and distributed, Although 70 organizations were targeted in this study, and only 35 questionnaires were filled and returned perhaps due to the sensitivity of the subject. The study found that The data security management of an organization has to find efficient and effective strategies to guarantee that they fully understand the information and data security risks affecting their operations, and implement apt controls to mitigate these risks. The security of organization's data and information assets is indispensable to ascertain and sustain confidence in their customers. This process has to maintain conformity with the legal requirements, and to shield the reputation of the organization. This procedure must be supported by operational and technical security standards to conduct active monitoring and assessments of their security program. The only prerequisite needed for a committed data security plan functioning effectively is strongly confirmed by the organization board of directors and the executive top management. The study recommended that organizations from the outset should have a set-plan, which has to be periodically analyzed, reviewed, and modified to keep abreast of the technological advancements and risks in order to protect electronic data.

13. Abu-Musa (2010)

The study titled "Information Security governance in Saudi organizations: an empirical study" sought to empirically examine the existence and implementation of information security governance (ISG) in Saudi organizations. A questionnaire was used to explore and evaluate the current status and the main features of ISG in the Saudi environment. A total of 167 valid questionnaires were collected and processed using the Statistical Package for Social Sciences. The results of the study revealed that although the majority of Saudi organizations recognize the importance of ISG as an integral factor for the success of IT and corporate governance, most of them have no clear information security strategies or written information security policy statements. The majority of Saudi organizations have no disaster recovery plans to deal with information security incidents and emergencies; information security roles and responsibilities are not clearly defined and communicated. The results also showed that alignment between ISG and the organization's overall business strategy was relatively poor and not adequately implemented. The results also showed that risk assessment procedures were not adequately and effectively implemented, ISG was not a regular item in the board's agenda, and there were no properly functioning ISG processes or performance-measuring systems in the majority of Saudi organizations.

14. Shing& Shing(2010)

The paper titled “Information Security Risk Assessment Using Markov Models” emphasized on how the likelihood of the risk propagates throughout the time and how to monitor the risk based on semi-Markov chain models this model starts with understanding what assets are potentially at risk, and then identifies what the possible threats are, and finally finds out what are the possible vulnerabilities that can be exploited. Markov chain model identifies threats in three categories (hardware, software, staff).The model has been applied in four states; it has been calculating the probability of threat occurrence numerically and expected losses .The study results were: the risk assessment can provide a way to protect the assets based on limited resources. Even though a risk assessment has been done and action has been taken to protect the assists, the risk assessment has to be updated due to environment change such as hardware, software or personnel changes. Therefore, risk assessment must be monitored all the time.The paper emphasize that this model is fit to risk assessment of information security, and reduce the economic cost, and stressed that the risk analysis a basic foundation to raise information security level.

15. **Somaini and Hazleton(2008)**

The paper titled "Information Security Management Programs: Organizational Assessment Lessons Learned and Best Practices Revealed" it was a series of papers showed that the preparation of information security strategy must be start with the evaluation process, and must take into account the fact that all information security management programs such as ISO 2700 and the other Focusing on the development of processes and the implementation of these stages carefully and do periodic revision, Based on this series of papers the Learned Lessons were:

- Lesson One: ISMS do not typically fail due to difficulty understanding or implementing technology
- Lesson Two: Comprehensive security policy is but one of the key building blocks to an effective ISMS
- Lesson Three: To successfully design an ISMP, the information security team must thoroughly understand the employee and management team's opinions, attitudes, and history with respect to enterprise information security
- Lesson Four: To successfully design an ISMP, the information security team must thoroughly understand the current state of operational processes and tools for IT infrastructure and application development

3.4 Comments on Previous Studies.

- This study has reviewed (15) studies, (4) local studies, and (10) Arabic and foreign studies.
  - The first group of studies have addressed the Information Security, which is second domain in this study, in order to reveal its dimensions, elements and its Influenced by these variables, some of these studies focused on factors of information security management (Altoom 2013,Kazemi et al 2011), other concerned with the implementation of information security governance as (Abu-Musa 2010), other focused on Reality of information security management as (Danaf 2013), while studies of(Hassan study 2013,Tayeh 2008) focused on effectiveness of information security management, the study of (Al-Awadi, & Saidani, 2010) Concerned with the awareness of the respondents to the data security risks.

- The second group of studies linked strategic planning with information security components. (Scanlan 2011) focused on The alignment of information security, strategic business, and strategic information System planning, (Abu-Musa 2010) focused on information security governance, while (Shing 2010) and (Somaini and Hazleton,2008) focusing on Information Security Risk Assessment, the (Derawi 2014) study was the closer study to the researcher study where the domains of (Derawi2014) exist within the second and third domain in the researcher study with a different study population, the researcher benefited from the Derawi (2014) study in some questions in the questionnaire.

- These studies were conducted in different environments, some of them were conducted in foreign environments and others were conducted in Arabic ones, as some of them were conducted in public sectors, and others were conducted in private sectors.
- These studies contributed in supporting the administrative development in the institutions and departments.
- The researcher, at the beginning, benefited from the previous studies in building the]vproposal, and determining the variable and the hypothesis of her study.
- These studies leaving the field wide and open for researchers to fill the research gaps and to contribute to the enrichment of the knowledge and practical sides of both domains of this search.
- The previous studies helped the researcher to develop the second section of the theoretical framework “information security”.
- Previous studies have helped the researcher to determine the appropriate statistical methods to analyze the study data, also in guiding to references and books to save time and effort. And make recommendations and proposals.

3.5 What distinguishes the current study from previous studies?

- It is unique study that examined the relationship between all phases of strategic planning and level information security in the governmental institutions "as the researcher found”.
- It highlights the ISSP environment, to increase the interest in it, and to issue the necessary recommendations to fill the gaps that hinder the effective implementation of the ISSP in the governmental institutions in Gaza.
- Previous studies examined the parts of the title of this study separately so these studies similar with it in some theoretical frameworks, but different in some things such as the dependent and associated independent variables, Society study, as well as the spatial domain and temporal.

- The current study used a multi regression model to show the impact ISSP on information security level, whereas most of previous research didn't use this model.

CHAPTER FOUR

RESEARCH METHODOLOGY

- Introduction
- Research Design
- Data Collection Resources
- Research Method
- Research Population
- Questionnaire Contents
- Pilot Study
- Questionnaire Validity
    - Arbitrators Validity
    - Internal Validity (internal consistency)
- Questionnaire Reliability
    - Statistical Methods

4.1 Introduction

This chapter describes the methodology steps that have been in this research, which addresses the research design, research Approach, research population, the sample that have been applied by the study, questionnaire design, pilot study, and statistical methods used in the data to arrive at results analysis and then achieving the objectives of the study.

4.2 Research Design

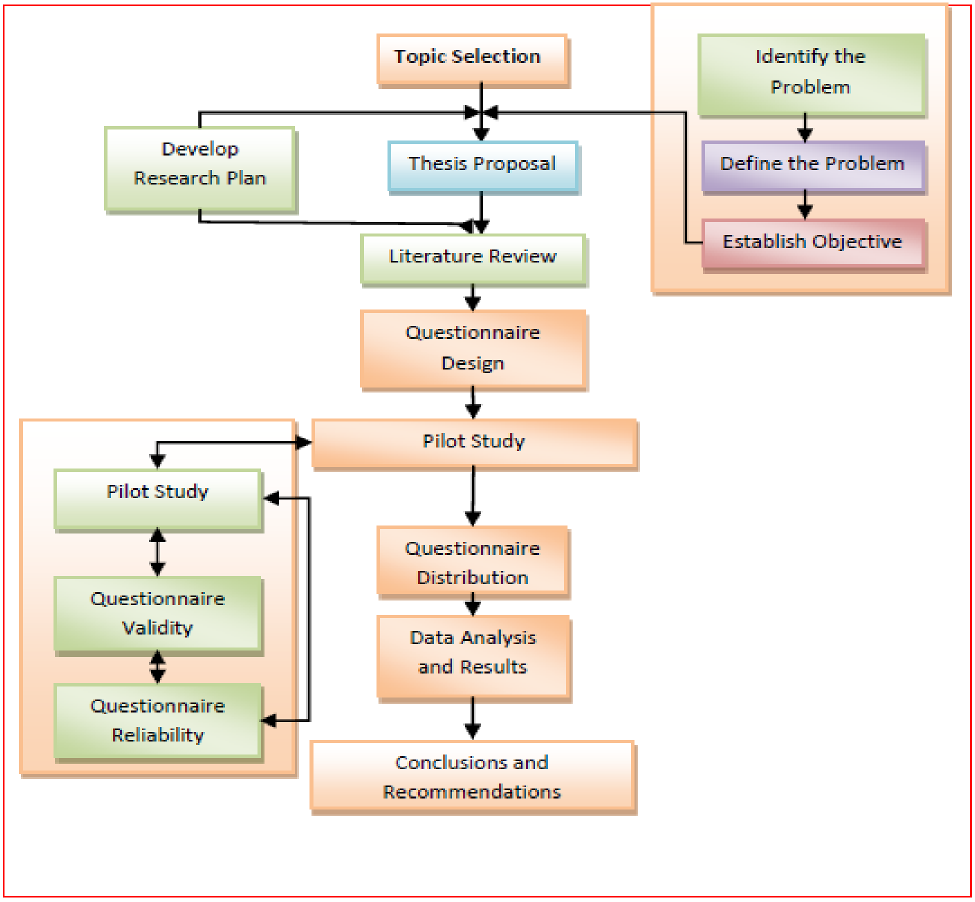


Figure (4.1) shows the research methodology flowchart, which leads to achieve its objectives.

By researcher relay on (Saunders, et al 2009)

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

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

The third phase included designing the study questionnaire to be used in examining the impact of strategic planning information security on the level of information security at the governmental institutions in Gaza.

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

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

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

The final phase includes the conclusion and recommendations.

4.3 Data Collection Resources

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

1. **Primary Resources**: in order to address the analytical aspects of the research theme, the research resorted to collect the primary data through the questionnaire as a main tool, which is designed especially to meet the research objectives. This questionnaire was distributed among the study population, (50) employees working at the governmental institutions in Gaza in order to get their opinions about examining the impact of strategic planning of information security on the level of information security at the governmental institutions in Gaza through the point of view managers and specialists.
2. **Secondary Resources:** in order to address the theoretical background of the study, it has been found on the secondary data collection resources, the likes of books, papers, essays, journals, research studies and reports that have handled the research theme and finally by surfing the internet to the related websites.

4.4 Research Method

This research has used the descriptive analytical method, which attempts to answer the basic question in the study "*The Impact of information security Strategic Planning on information security Level at the Governmental Institutions in Gaza Through The Perspective of Managers and Specialists*", and what the nature of the Phenomenon which is research theme., and analysis of the phenomenon, its environment, and clarifying the relationship between its components. The description is given mainly by units, conditions, relationships, groups, categories, or patterns that do exist. Also include related opinions and trends about it, as well as the operations contained and the resulting effects. The descriptive approach extends to addressing how the phenomenon works. This approach satisfies the research goals in order to compare and evaluate the results, raising our hopes to publicize a meaningful content to support the available knowledge of the research theme.

4.5 Research Population And Sample Size

The study' population is the Governmental Institutions in Gaza" the Ministry of Telecommunications and Information Technology and the Ministry of Interior and National Security". The research has focused on managers and the staff of information technology, information archiving and planning departments in those institutions because it discussed the information security from a managerial perspective. This population consists of (57) employees.

The Study Sample: the sample was 50 employees, according to Retched Gerger formulation **n=(((z/d)2)*(0.50) 2)/(1 +((1/N)*((((z/d)2)*(0.50) 2))-1))**

(N= study' population, Z: confidence level at 95% (standard value of 1.96),E:error proportion ≤0.05)

Table (4.1) Research Population's Governmental Institution Representation

Governmental Institution	Frequency	Percent (%)
Ministry of Telecommunication and Information Technology	29	58
Interior and National Security Ministry	21	42
Total	50	100.0

4.6 Questionnaire Contents

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 questions: 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 *The Impact Of information security Strategic Planning On information security Level ,through the Perspective of Managers and Specialists of Information System* "as follows

First section: personal data consist of) age, gender, experience, training, job title, job field, qualification)

Second section: related to The Impact Of information security Strategic Planning On information security Level ,Through The point Of View Managers and Specialists Of Information System, consist of (78) Sentences and divided into six fields as follows

1. First Domain: clarity of Information Security concept and awareness of importance of strategic planning for information security**,**consist of (10) Sentences
2. Second Domain: information security environment analysis**,** consist of 12 Sentences
3. Third Domain: The formulation of the strategic plan for information security**,**consist of (15) Sentences
4. Fourth Domain: Implementation of the strategic plan for information security, consist of (11) Sentences.
5. Fifth Domain: Control and monitoring of the application of the Strategic Plan,consist of (11) Sentences
6. Sixth Domain: Level of information security, consist of (19) Sentences.

The questioner was distributed in Arabic language because most of the targeted population members are unfamiliar enough with English language.

4.6.1 Data Measurement

In order to be able to select the appropriate method of analysis, the level of measurement must be understood. For each type of measurement, there is/are an appropriate method/s that can be applied and not others. In this research, scale 1-10 is used.

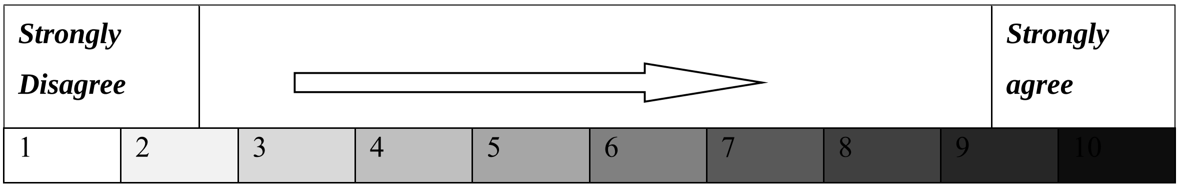


Figure 4.2 **Measurement scale**

4.7 Questionnaire Validity

Validity refers to the degree to which a questionnaire measures what it is supposed to be measuring. High validity is the absence of systematic errors in the evaluating questionnaire. When a questionnaire is valid; it truly reflects the concept it is supposed to measure. (George, & Mallery 2006).

4.7.1 Arbitrators Validity

This group of experts actually were of the academic staff of the Faculty of Commerce, the Faculty of Engineering and Information Technology, the Scientific Research Deanship, from the Islamic University and Al_Azhar university in Gaza. Those arbitrators had issued their suggestions around the questionnaire and its appropriateness to achieve the study objective. In addition, an expert in statistics was requested to evaluate that the used questionnaire is statistically valid and was designed well enough to provide the relations and tests between the study variables. The names and some information about the arbitrators are explained in Appendix (A). The experts agreed that the questionnaire was valid and suitable enough to be used with some amendments. The arbitrators ‘suggestions and amendments were taken into consideration in order to set the appropriate questionnaire as shown in Appendix (B).

4.7.2 Internal Validity

Internal validity of the questionnaire was evaluated after conducting a pilot study by an exploratory sample, which consisted of 25 questionnaires, by measuring the correlation coefficients between each item in one field and the whole filed.

Table (4.2)

The correlation coefficient between each item (question) in the field and the whole field

First Domain			**Second Domain**		
Item No	**Pearson ion coefficient**	**Sign**	**Item No**	**Pearson correlation coefficient**	**sign**
1	0.867	**0.000	**1**	0.478	*0.024
2	0.881	**0.000	**2**	0.817	**0.000
3	0.774	**0.000	**3**	0.832	**0.000
4	0.802	**0.000	**4**	0.892	**0.000
5	0.939	**0.000	**5**	0.944	**0.000
6	0.862	**0.000	**6**	0.935	**0.000
7	0.784	**0.000	**7**	0.955	**0.000
8	0.828	**0.000	**8**	0.898	**0.000
9	0.856	**0.000	**9**	0.592	**0.004
10	0.570	**0.006	**10**	0.837	**0.000
			11	0.734	**0.000
			12	0.741	**0.000
Third Domain			**Fourth Domain**		
Item No	**Pearson correlation coefficient**	**Sign**	**Item No**	**Pearson correlation coefficient**	**Sign**
1	0.838	**0.000	1	0.924	**0.000
2	0.806	**0.000	**2**	0.893	**0.000
3	0.873	**0.000	**3**	0.877	**0.000
4	0.918	**0.000	**4**	0.879	**0.000
5	0.854	**0.000	**5**	0.862	**0.000
6	0.806	**0.000	**6**	0.878	**0.000
7	0.829	**0.000	**7**	0.670	**0.000
8	0.828	**0.000	**8**	0.845	**0.000

First Domain			Second Domain		
Item No	**Pearson ion coefficient**	**Sign**	**Item No**	**Pearson correlation coefficient**	**sign**
9	0.880	**0.000	**9**	0.778	**0.000
10	0.812	**0.000	**10**	0.770	**0.000
11	0.908	**0.000	**11**	0.858	**0.000
12	0.856	**0.000			
13	0.885	**0.000			
14	0.819	**0.000			
15	0.915	**0.000			
Fifth Domain			**Sixth Domain**		
Item No	**Pearson correlation coefficient**	**Sign**	**Item No**	**Pearson correlation coefficient**	**Sign**
1	0.932	**0.000	**1**	0.783	**0.000
2	0.945	**0.000	**2**	0.892	**0.000
3	0.931	**0.000	**3**	0.869	**0.000
4	0.890	**0.000	**4**	0.879	**0.000
5	0.899	**0.000	**5**	0.837	**0.000
6	0.696	**0.000	**6**	0.822	**0.000
7	0.949	**0.000	**7**	0.953	**0.000
8	0.903	**0.000	**8**	0.963	**0.000
9	0.933	**0.000	**9**	0.929	**0.000
10	0.841	**0.000	**10**	0.937	**0.000
11	0.961	**0.000	**11**	0.823	**0.000
			12	0.941	**0.000
			13	0.913	**0.000
			14	0.827	**0.000
			15	0.910	**0.000
			16	0.968	**0.000
			17	0.912	**0.000
			18	0.910	**0.000
			19	0.880	**0.000

**Indicates Correlation Significance at $\alpha \leq 0.05$

Results described in the Table (4.2) shows that the paragraphs of the questionnaire have a strong correlation coefficients and statistically significant at the level less than (0.05), this indicates that the questionnaire enjoying by high sincerity.

4.8 Reliability :

Reliability of a questionnaire is the degree of consistency in which it measures the level of consistency of the questionnaire results if it will be distributed several times under the same conditions. In other words, questionnaire reliability means that the questionnaire will give the same results if it will be distributed several times to the study sample in specific time periods. For the most purposes reliability coefficient above 0.7 is considered satisfactory (George and Mallery, 2006).

To measure the reliability can be achieved by using Cronbach's Alpha Coefficient and Half Split Method through the SPSS software .

4.8.1 Cranach's Alpha Coefficient:

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 Cranach's coefficient alpha value between (0.0) and (+ 1.0), and the higher values reflects a higher degree of internal consistency. (George and Mallery, 2006)

Table (4.3) for Reliability Cronbach's Alpha

All Domains	No. of Items	Cron. Alpha
	78	0.988
First Domain: clarity of Information Security concept and awareness of importance of strategic planning for information security	10	0.928
Second Domain: information security environment analysis	12	0.951
Third Domain: The formulation of the strategic plan for information security	15	0.973
Fourth Domain: Implementation of the strategic plan for information security	11	0.957
Fifth Domain: Control and monitoring of the application of the Strategic Plan	11	0.976
Sixth Domain: Level of information security	19	0.985

Table No. (4.3) shows the Cronbach's coefficient alpha was calculated and the results were in the range from 0.928 and 0.985, and the general reliability for all items equal 0.988 this range is high; the result ensures the reliability of the questionnaire.

4.8.2 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

Table (4.4) Split-Half Coefficient method

Questionnaire	person-correlation	Spearman-Coefficient
	0.729	0.843
First Domain: clarity of Information Security concept and awareness of importance of strategic planning for information security	0.825	0.904
Second Domain: information security environment analysis	0.884	0.939
Third Domain: The formulation of the strategic plan for information security	0.892	0.943
Fourth Domain: Implementation of the strategic plan for information security	0.753	0.860
Fifth Domain: Control and monitoring of the application of the Strategic Plan of information security.	0.948	0.973
Sixth Domain: Level of information security	0.972	0.986

As shown in Table No.(4.4), all the corrected correlation coefficients values are between 0.860and 0.986and the general reliability for all items equal 0.843, this result ensures the high reliability of the questionnaire.

4.9 Statically Method

To achieve the research goal, researcher used the statistical package for the Social Science (SPSS) for manipulating and analyzing the data. The following statistical tests were used to analyze the data and the study hypothesis:

I. Frequencies, means and percentages to represent the collected data in meaningful figures.

II. Pearson Correlation Coefficient was used to measure the correlation between two variables, where it was applied to test the questionnaire validity.

III. Cronbach's Alpha coefficient was used to test the questionnaire reliability.

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

V. T-test is used to determine if the mean of a paragraph is significantly different from a hypothesized value 6. If the P-value (Sig.) is smaller than or equal to the level of significance, $\alpha = 0.05$ then the mean of a paragraph is significantly different from a hypothesized value 6. The sign of the Test value indicates whether the mean is significantly greater or smaller than hypothesized value 6. On the other hand, if the P-value (Sig.) is greater than the level of significance, $\alpha = 0.05$, then the mean a paragraph is insignificantly different from a hypothesized value 6.

VI. The Pearson Correlation Coefficient test was used to examine the correlation significance in testing the first main hypothesis.

VII. The Two-independent samples T Test was used to determine if there are differences indicating statistical significance between the means of two groups of data like the respondents ‘gender (male and female).

VIII. The One-Way ANOVA test was used to determine if there are differences indicating statistical significance between the means in the case of three groups of data and more like the respondents ‘qualification (general secondary, diploma, bachelor and master).

CHAPTER FIVE
DATA ANALYSIS AND DISCUSSION

- Introduction
- Normality Distribution Test
- Data Analysis
  - Personal information
  - Study Fields Analysis
- Hypothesis Testing

5.1 Introduction:

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

5.2 Normality Distributing Test

One Sample Kolmogorov-Smirnov test was used to identify if the study questionnaire data follows the normal distribution or not, this test is considered necessary in the case of testing hypotheses as most Parametric Tests stipulate data to be normally distributed (Henry, C. and Thode, Jr., 2002).

Table (5.1)
One Sample Kolmogorov-Smirnov Test

	Z-value	sig.
First Domain: Clarity of Information Security concept and awareness of importance of strategic planning for information security	**0.147**	**0.200**
Second Domain: Information security environment analysis	**0.140**	**0.252**
Third Domain: The formulation of the strategic plan for information security	**0.151**	**0.190**
Fourth Domain: Implementation of the strategic plan for information security	**0.163**	**0.183**
Fifth Domain: Control and monitoring of the application of the Strategic Plan	**0.138**	**0.199**
Sixth Domain: Level of information security	**0.130**	**0.192**
Total	**0.153**	**0.198**

Through table (5.1) it is clear that the level of significance greater than 0.05 for each domain, and this shows that the data follow a normal distribution and must use parametric tests.

5.3 Data Analysis:

5.3.1 Personal information

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

1. **Qualification:**

Table (5.2) Research sample’s Job Qualification Representation

Qualification	Frequency	Percentage
B.Sc	32	64
Higher Studies	18	36
Total	50	100.0

Table No.(5.2) shows that 64% of the sample of qualification are " B.Sc ", and 36% of the sample of qualification are " Higher Studies ". The presence of 36% “Higher Studies” Could be attributed to the importance of information security strategic planning so the government institutions took into their account the existence of a class of highly qualified staff as a part of those who are treating this topic.

2. **Specialization:**

Table (5.3)Research sample’s specialization Representation

Specialization	**Frequency**	**Percent (%)**
Computer Engineering	20	40
IT	16	32
Business Administration	3	6
Other	11	22
Total	50	100.0

Table (5.3) shows that 72% of the study's sample are specialized in the field of computers, that is attributed to the government attempt to enhance the IT units in order to achieve remarkable steps towards the successful launch of information security, the presence of 22% " others" is attributed to the fact that there are staff contributed in the security of information process or its strategic planning but their field is not related with computer such as lawyers.

3. **Age**

Table (5.4) Research sample’s age Representation

Age	**Frequency**	**Percent (%)**
Less than 30 years	9	18
30-40 years	38	76
40-50 years	1	2
More than 50	2	4
Total	50	100.0

Table (5.4) shows (94%) of the study sample is in the young category this percentage is attributed to the fact that the government ministries interest to presence of a young energies able to keep up technological development, also table (5.4) shows 6% more than 40 that reflects the youth participation among the work force and it could be concluded that the IT body is youth and capable to exert the best in its career. This result is attributed to the fact that IT generation is relatively new and becomes an essential part of our contemporary life.

4. Gender

Table (5.5) Research sample's gender Representation

Gender	Frequency	Percent (%)
Male	40	80
Female	10	20
Total	50	100.0

Table (5.5) shows that 80% of the study sample are males and 20% are females which is approximately equal to the ratio of the female workforce in Gaza, "19.7," according to a report by the Palestinian Center for Statistics (PCBS) on (11-7- 2015). This result normal depending on the prevailing belief in government institutions in the Palestinian society that males better able to work in the field of computer, and they have the ability to work under pressure more than females.

5. Job Title

Table (5.6) Research sample's Job Title Representation

Job Title	Frequency	Percent (%)
General Manager	4	8
Chief Department	12	24
Chief Branch	11	22
Engineer	15	30
Programmer	6	12
Other	2	4
Total	**50**	**100.0**

Table (5.6) shows that 42% of the study sample job title in the field of computer, and 8% Director General, while the chief of department and director of the department (46%) This reflects the diversity of job titles among the respondents.

6. Experience

Table (5.7) Research Sample's Experience Representation

Experience	Frequency	Percent (%)
Less than 5	12	24
5-10	27	54
More than 10 year	11	22
Total	50	100.0

Results in table (5.7) indicates that 78% of the study sample who have experience in the field of work (less than 10 year) this result is attributed to the government efforts to fill the available vacancies after the Palestinian division events.

7. Work field

Table (5.8) Research Sample's Work field Representation

work field	Frequency	Percent (%)
Enterprise Management, And drawing plans, policies and strategies	7	14
Developing Software Applications	15	30
Developing Databases Applications	9	18
Operating systems and networks	7	14
Other	12	24
Total	50	100.0

The result in table(5.8) shows that the (52%) of the sample work in information technology field and 14% work in enterprise management, and drawing plans, policies and strategies. This result is attributed to fact that the study revolves around information security and the specialized computer's category is the most knowledge by preserved methods, however, the strategic planning process itself needs a special category with full knowledge of its steps and methods.

8. Training for strategic planning of information security

Table (5.9) Research Sample's courses (strategic planning of information security) Representation

No of courses	Frequency	Percent (%)
No training	25	50
1-3 course	25	50
Total	50	100.0

Table (5.9) shows that 50% of the study sample said they did not take any strategic planning for information security courses, and 50% said that the number of courses to strategic planning for the security of information ranging from one to three. This result is attributed to the presence of interest at government institutions to train some of its staff in the area of strategic planning for information security according to provide opportunities, and to government budgets.

9. Training for information security

Table (5.10) (Information security courses)

Courses	Frequency	Percent (%)
No course	20	40
1-3	27	54
4-6	3	6
Total	**50**	**100.0**

Table (5.10) shows that 40% of the study sample said they did not take any strategic planning for information security courses, and 60% have courses to security of information ranging (1-6), This result is attributed to the presence of interest at government institutions to train its staff in the area of information security according to provide opportunities, and to government budgets.

10. Respondents' Governmental Institution:

Table **(5.11)Research Population's Governmental Institution Representation**

Governmental Institution	Frequency	Percent (%)
Ministry of Telecommunication and Information Technology	29	58
Interior and National Security Ministry	21	42
Total	50	100.0

Table (5.11) shows that 58% of study sample works at Ministry of Telecommunication and Information Technology and 42% Interior and National Security Ministry. This is because the Ministry of Communication is the estuary to all ministries electronically which issue information security policies.

5.3.2 Study Fields Analysis

In order to answer the study questions "What is the effect of strategic planning for information security at the level of information security through the perspective of managers and specialists in government institutions?" The researcher used the One-Sample T test mean and P-value (sig.) for each domain.

5.3.2.1 First Domain: The clarity of Information Security concept and awareness of importance of strategic planning for information security

Table (5.12): The respondents' opinions towards the items of the first domain

#	Question	mean	Weight mean%	Value (t)	Sig	Rank
1	The higher administration is aware that Information Security is an important part of the institution's security	7.580	75.8	7.115**	0.000	2
2	The administration is aware and convinced that strategic planning for Information Security is essential in strategic planning of the whole institution	7.360	73.6	7.711**	0.000	3
3	The Higher Administration is convinced that any violation of information and any defects in its security will lead to disrupting the institution's general aims	8.040	80.4	8.930**	0.000	1
4	There is a special team for strategic planning of Information Security comprising administration and IT specialists	4.960	49.6	6.552**	0.000	8

#	Question	mean	Weight mean%	Value (t)	Sig	Rank
5	The managers and Information Systems' specialists are aware that strategic planning increases confidence among the workers	6.720	67.2	6.859**	0.000	7
6	Information Security specialists clearly understand that Information Security problems must be solved strategically not technically only	6.720	67.2	6.729**	0.000	7
7	There is a complete understanding that Information Security is not limited to computer security but includes individuals', equipment's, buildings', and data, and all of this needs executive plans and policies to protect them	7.060	70.6	6.266**	0.000	4
8	There is awareness that strategic planning decreases economic expenses	7.000	70	7.000**	0.000	5
9	There is awareness that strategic planning guarantees good use of capabilities, resources, and outside opportunities and contributes to eradicating weaknesses	6.980	69.8	6.747**	0.000	6
10	There is a training program specific to increasing awareness of the importance of strategic planning for Information Security	4.640	46.4	4.365*	0.02	9
All items		6.706	67.06	6.827**	0.000	

The following result could be concluded:

The mean of responses to all paragraphs in this domain is between (4.64%-8.04%) with weight mean (46.4-80.4)According to the gradient scale decimal and the weight mean of first domain equal " 67.06%" with sig. (p-value) equals (0.000) less than (α = 0.05), which shows statistical significance and that the response level of this domain is greater than the neutrality degree of (6). This indicates that the respondents agreed with the domain “*The clarity of Information Security concept and awareness of importance of strategic planning for information security”*

- **Results in the table show that the top three paragraphs are:**
  - Item No. (3)" The Higher Administration is convinced that any violation of information and any defects in its security will lead to disrupting the institution's general aims " the weight mean equal " 80.4%" and ranked equal " 1"
  - Item No(1) “The higher administration is aware that Information Security is an important part of the institution's security” the weight mean equal " 75.8%" and ranked equal "2"
  - Item No (2) “The administration is aware and convinced that strategic planning for Information Security is essential in strategic planning of the whole institution” the weight mean equal " 73.6%" and ranked equal " 3".

- **The lowest three paragraphs are:**
  - Item No(5) “The managers and information systems' specialists are aware that strategic planning increases confidence among the workers**”** and Item No(6)” Information Security specialists clearly understand that information security problems must be solved strategically not technically only” the weight mean equal " 67.2%" and ranked equal " 7".
  - Item No(4) “There is a special team for strategic planning of Information Security comprising administration and IT specialists**”** the weight mean equal " 49.6%" and ranked equal " 8".
  - Item No(10) “There is a training program specific to increasing awareness of the importance of strategic planning for information security**”** the weight mean equal " 46.4%" and ranked equal " 9".

The results above denote the following facts:

- The approval of first domain “clarity of the concept of information security and awareness of its importance” is 67.06%. it is moderately rate, this implies that there is awareness of the importance of strategic planning for the security of information in the governmental institutions but there is a need to increase awareness of this.
- There is an excellent approval degree(80%) of respondents‘ opinions towards "the existence of conviction among management that any violation of the information will lead to obstructing the organization's objectives," and that information security is a part of the organization's security and strategic planning for information security a key part of the strategic planning of the entire organization, This high approval is an evidence of the presence of a clear concept for Information security, and awareness of the importance of strategic planning for it.
- There is good approval degree of respondents ‘opinions (70-75.8) towards “the information security exceeds the computer problems, information security problems should be resolved strategically and not just technical, strategic planning for information security works to reduce the economic cost, the elimination of any weaknesses in the organization, and promotes optimum utilization of resources in the enterprise." This level of approval confirms the existence awareness of the importance of strategic planning for information security at government institutions. This result is attributed to occurrence of some violations in government institutions and it was handled technically but the technical solution does not provide a fundamental solution to the problem.
- The results show that there is a weak degree approval of respondents ‘opinions towards items " There is a special team for strategic planning of Information security comprising

administration and IT specialists ", "the existence of training program specific to increasing awareness of the importance of strategic planning for Information Security." The researcher’s opinion is due to the weakness of the budgets in the governmental institutions and the volatile political situation.

- The result agreed with the study of Derawi (2014) and Danf (2013) where they have found in their study that the administration in the Palestinian universities realize the importance of information security as part of the enterprise security, also agreed with Tom study partly (2014) “that there is weakness in the training of staff universities in the field of information security”, also agreed with (Scanlan, 2011) study in part “It must be planned for the security of information strategically “, agreed with Abu-Musa(2010) that “ the Saudi institutions have a high degree of awareness of the importance of information security” in researcher view, this agreement is due all respondents in those studies are IT specialists or work with information security so they have the approximately the same scientific culture.
- The result agreed with what Shlii(2011) found “There is awareness of civil defense officers in Saudi Arabia that Strategic planning reduces the damage of disasters, the agreement in this part due

5.3.2.2 **Second domain:** Information security environment analysis.

Table (5.13) The respondents’ opinions towards the items of the second domain

#	Question	mean	Weight mean %	Value (t)	Sig	Rank
1	The internal and external environment analysis is considered a fundamental pillar in strategic planning of Information Security	7.820	78.2	11.23**	0.000	1
2	There is a specialized team for the internal and external IT environment analysis	4.640	46.4	2.02*	0.012	12
3	Several tools are used in the analysis process to get the most accurate results	4.720	47.2	2.23*	0.012	11
4	Through the analysis process, information is categorized and the basic information is focused on	5.440	54.4	4.45**	0.000	10
5	Power center of Information Security are identified objectively in order to be employed in the organization	5.560	55.6	4.61**	0.000	9

#	Question	mean	Weight mean %	Value (t)	Sig	Rank
6	Through environmental analysis, internal and external threats are identified objectively	5.900	59	5.76**	0.000	4
7	Possibility of any violation caused by threats is truthfully identified	5.760	57.6	5.11**	0.000	7
8	Risk intensity caused by any threats is identified (disrupted equipment – human or natural disasters) effectively	5.600	56	5.22**	0.000	8
9	Weakness or strength of human and financial resources as well as the organizational structure affects the Information security environmental analysis	7.360	73.6	11.12**	0.000	2
10	Socio-politico-economic and legal aspects are considered while doing an Information security environmental analysis in the institution	5.960	59.6	5.62**	0.000	3
11	Features and resources necessary for success are defined and developed	5.880	58.8	5.59**	0.000	5
12	There is an information system helping to obtain the internal and external environment information	5.820	58.2	5.26**	0.000	6
All items		5.872	58.72	5.69**	0.000	

The responses of the study sample toward second domain show the following results:

The mean of responses to all paragraphs in this domain is between (4.64%-7.82%) with weight mean (46.4-78.2) according to the gradient scale decimal, the weight mean for second domain equal (58.72%) and the sig. (p-value) equals (0.00) less than (α = 0.05), which shows statistical significance and that the response level of this item does not differ significantly than the neutrality degree of (6). This indicates that the respondents agreed with the domain *"Information security environment analysis"*

The top three paragraphs are:

- Item No. (1)" The internal and external environment analysis is considered a fundamental pillar in "strategic planning of Information Security " the weight mean equal " 78.2%" and ranked equal " 1"
- Item No(9) "Weakness or strength of human and financial resources as well as the organizational structure affects the Information security environmental analysis" the weight mean equal " 73.6%" and ranked equal " 2"

- Item No(10) “Socio-politico-economic and legal aspects are considered while doing an Information security environmental analysis in the institution " 59.6%" and ranked equal " 3".

- **The lowest three paragraphs are:**
  - Item No(4) " Through the analysis process, information is categorized and the basic information is focused on" the weight mean equal " 54.4%" and ranked equal " 10".
  - Item No(3) " Several tools are used in the analysis process to get the most accurate results" the weight mean equal " 47.2%" and ranked equal " 11".
  - Item No(2) " There is a specialized team for the internal and external IT environment analysis" the weight mean equal " 46.4%" and ranked equal " 12".

The results above denote the following facts:

- The weight mean of second domain “*information security environment analysis”* is 58.72%. it is less than moderately rate (does not differ significantly than 60%) that implies there is weakness in the governmental institutions information security environment analysis, the researcher attributed this result to what found in domain one the employees have no enough training about information security strategic planning, Add to that the environmental analysis process need equipment and machinery and financial situation of government institutions are not allowed to do that. Also, most government institutions rely to solve security problems technically rather than look at the threats and strengths and weaknesses. Therefore, government institutions should pay more attention to information security environmental analysis according available budgets and it should be allocated of teams for this process.

In detail,

- There is high degree approval of respondents' opinions 78% on the paragraph "Is the internal environment and external analysis of the basic foundation for strategic planning for information security, "`and this indicates that the sample members have awareness of the importance of environmental analysis for the security of information, but the circumstances and the equipment does not help.

- There is good approval degree of respondents ‘opinions (73%) towards "Weakness or strength of human and financial resources as well as the organizational structure do affect the Information security environmental analysis." This result is evidence of the results of other items to this domain where the government institutions have weakness in the training of human resources, and weak budgets and thus lead to weakening environmental analysis.

- There is a moderately approval degree (59.6 % does not differ significantly than 60%) of respondents ‘opinions towards two items which contained on “The political and economic aspects are taken into account in the process of environmental analysis, internal and external threats are determined objectively."

- The approval degree is less than moderately (50%-59%) of respondents opinions towards items which contained on “Through the analysis process, information is categorized and the basic information is focused on, Possibility of any violation caused by threats is truthfully identified, Features and resources necessary for success are defined and developed, Risk intensity caused by any threats is identified, There is an information system helping to obtain the internal and external environment information” Researcher attributed the results to weakness of training and a lack of specialized teams to analyze information security environment.

- There is low approval degree(less than 50) of respondents opinions towards the remaining paragraphs “There is a specialized team for the internal and external IT environment analysis, several tools are used in the analysis process to get the most accurate results”.

- The finding agreed with Abu-Musa(2010) where the degree of approval among respondents towards "Saudi Arabia institutions analyze and identify and evaluate the risks and have the information systems helps in the analysis process” in Abu-Musa(2010) study was less than moderately. Also agreed with Salah(2011) and Somaini & Hazleton(2008) which considered a risk analysis is one of the bases for the management of information security. The agreement in this paragraph is due to the fact that the sample in studies is computer specialists, although they have awareness of the importance of risk identification, but they are actually solving the problems technically rather than strategically.

- The finding agreed with Awadi & Saidani (2010) study where it found high approval (90%) towards “Strategic planning is based on the analysis of the surrounding this is due the culture of the respondents where a good number of them, have experience in administrative sciences
- The study disagreed with Dirawi (2014), where the degree of approval toward "Palestinian universities interested in the process of environmental analysis at strategic planning for information systems" was good (74%). And disagreed with Sahli(2011), Where civil defense officers’ opinion in Saudi Arabia gave a high percentage of approval on "the use of environmental analysis at strategic planning for disaster damage

reduction". All those disagreement have one reason that is the nature of the work in government institutions, which is linked to government budgets and weakness of training.

5.3.2.3 Third domain: The formulation of the information security strategic plan:

Table (5.14):The respondents' opinions towards the items of the third domain

#	Question	mean	Weight mean%	Value (t)	Sig	Rank
1	There is a clear, time-limited vision to achieve them	5.540	55.4	4.19**	0.000	13
2	Strategic vision of Information Security reflects the high level of Information Security	6.460	64.6	7.69**	0.000	1
3	The institution has a clear mission about information security that can be altered into plans and policies	6.200	62	6.81**	0.000	4
4	Objectives (purposes) of Information Security are set according to environmental analysis results	5.540	55.4	5.07	0.000	14
5	The Information Security's mission and objectives are related with the management information systems' mission to support and complete the culture and institution's message in order to achieve the objectives	6.160	61.6	7.07**	0.000	6
6	Strategic plans for Information Security is formulated to achieve the Confidentiality, Integrity, Availability of the information to the authorized entities at the right time	6.180	61.8	6.75**	0.000	5
7	Strategic plan for Information security includes identifying responsibilities and obligations for all workers	6.140	61.4	7.72**	0.000	7
8	The required resources are identified to objectively implement the plan	6.040	60.4	7.04**	0.000	8
9	Strategic planning for Information security is formulated to include all constituent of Information security	6.020	60.2	6.21**	0.000	10
10	Strategic planning for Information security is formulated in accordance with international criteria	5.240	52.4	3.89**	0.000	15
11	Alternative plans are prepared to deal with possible environmental changes	5.800	58	5.44**	0.000	12
12	Any change in the institution's strategy is followed by a change in information security policies	6.040	60.4	6.39**	0.000	8
13	Information security policies are clear, easy-to-understand, and flexible in dealing with all requirements	6.440	64.4	8.17**	0.000	2
14	Strategic alternatives are compared to take the best in terms of cost, available resources, and achieving the objectives	6.260	62.6	7.48**	0.000	3

15	All IT specialists And administrators who are involved in information security participate In the formulation of the strategic plan	5.820	58.2	5.22**	0.000	11
All items		5.992	59.92	6.34**	0.000	

The responses of the study sample toward third domain show the following results:

The table (5.14) shows that the mean of responses to all paragraphs in this domain is (5.24-6.46) with weight mean (52.4%-64.6%) according to the gradient scale decimal. The weight mean for the third domain equal (59.92%), and the sig. (p-value) equals (0.000) less than ($\alpha = 0.05$), which shows statistical significance and that the response level of this domain does not differ significantly than the neutrality degree of (6) This indicates that the respondents agree with the domain *"The formulation of the information security strategic plan"*

- **The top three paragraphs are:**
  - Item No. (2)" Strategic vision of Information Security reflects the high level of Information Security" the weight mean equal " 64.6%" and ranked equal " 1"
  - Item No(13) "Information security policies are clear, easy-to-understand, and flexible in dealing with all requirements "the weight mean equal " 64.4%" and ranked equal " 2"
  - Item No(14) "Strategic alternatives are compared to take the best in terms of cost, available resources, and achieving the objectives " the weight mean equal " 62.6" and ranked equal " 3".
- **The lowest three paragraphs are:**
  - Item No (1) " There is a clear, time-limited vision to achieve them " the weight mean equal" 554.%" and ranked equal " 13".
  - Item No(4) " Objectives (purposes) of Information Security are set according to environmental analysis results" the weight mean equal "47.2%" and ranked equal "13".
  - Item No (10)" Strategic planning for Information security is formulated in accordance with international criteria "the weight mean equal"52.4%" and ranked equal "15".

The results above denote the following facts:

The approval toward third domain is 59.9%. It is moderately rate, this implies that there is interest in government institutions to the process of formulating a strategic plan for information security, but not the extent required. This result is attributed to the economic and political conditions that affect the effectiveness of the performance of employees in government organizations, as well as the fact that most specialists in information security are a modern category need more training.

In detail,

- The approval of the respondents is moderately degree (59%-69) on most of the paragraphs that contain " *The Information Security's mission and objectives are related with the management information systems' mission to support and complete the culture and institution's message in order to achieve the objectives*, Information *security policies are clear, easy-to-understand, and flexible in dealing with all requirements*" the researcher attributed this result to lack of training in strategic planning for information security**.**

- There is less than moderately degree of approval of respondents ‘opinions (less 59) towards " There is a clear vision to achieve them, Strategic planning for Information security is formulated in accordance with international criteria, Objectives (purposes) of Information Security are set according to environmental analysis results " this result related with second domain where there is weakness in environment analysis to it difficult to build objective and clear vision based on the analysis.

- The finding of study disagreed with Dirawi(2014) where he viewed mission in separate domain of his study and he found the approval degree in Palestinian universities toward "mission " was good(74%).and disagreed with Sahli(2011)"Where civil defense officers' opinion in Saudi Arabia gave a high percentage of approval on "formulating strategic plan for disaster damage reduction". The difference return to core of studies which search about strategic planning for all organization not about ISSP also the sample that their qualification related to the science of administration.

- The finding agreed with Abu-Mousa(2010) in low degree of approval towards formulate plans and the existence of a written mission and objectives(Noting that the difference of study population), Also this study agreed with Al-wadi& Saidani (2010) in low degree of approval toward" formulation a plan for information security". In those studies the plane information security and that is relatively new issue, the respondents have no enough experience to deal with it strategically.

5.3.2.4 Forth Domain: Implementing of the Information Security Strategic Plan.

Table (5.15)The respondents' opinions towards the items of the fourth domain

#	Question	mean	Weight mean %	Value (t)	Sig	Rank
1	The set plan simply and without any complications is converted into programs, activities, and procedures	5.680	56.8	4.96**	0.000	5
2	There are clear and identified annual operational plans specific to Information Security level to achieve the objectives required	5.580	55.8	4.28**	0.0000	7
3	The institution has an operational plan to achieve annual objectives	7.060	70.6	8.35**	0.000	1
4	The procedures set in strategic plan are implemented by all employees each according to his/her responsibilities	6.440	64.4	6.97**	0.000	2
5	The identified activities are implemented on time	5.660	56.6	5.68**	0.000	6
6	The activities are set in accordance with the identified objectives and purposes, taking into consideration the changing environmental conditions	5.800	58	5.73**	0.000	4
7	There is a incentives system for workers to encourage them to implement the plans and reach the required targets	4.300	43	2.02*	0.012	11
8	The identified activities include all aspects specific to Information security (Individuals, equipment, and networks)	5.860	58.6	6.04**	0.000	3
9	The institution has an effective administration, and leaders encouraging the employees to implement the activities and achieve the objectives	5.460	54.6	4.80**	0.000	8
10	Enough budget is given to help implement the plans	5.120	51.2	3.27**	0.000	9
11	Certain programmers are identified to help in the implementation process	5.100	51	3.39**	0.000	10
All items		5.642	56.42	5.05**	0.000	

The responses of the study sample toward fourth domain show the following results:

The mean of responses to all paragraphs in fourth domain is between (4.30%-7.06%) with weight mean (43 -70.6) According to the gradient scale decimal, The weight mean for fourth domain equal (56.42%) and the sig. (p-value) equals (0.000) less than (α = 0.05), which shows statistical significance and that the response level of this domain is less than the neutrality degree of (6). This indicates that the respondents disagreed with the domain *"The Implementing of the Information Security Strategic Plan"*

- **The top three paragraphs are:**
  - Item No. (3)" The institution has an operational plan to achieve annual objectives" the weight mean equal " 70.6%"   and ranked equal " 1"
  - Item No(4) "The procedures set in strategic plan are implemented by all employees each according to his/her responsibilities" the weight mean equal " 64.4%"   and ranked equal " 2"
  - Item No(8)" The identified activities include all aspects specific to Information security (Individuals, equipment, and networks)"the weight mean equal " 58.6."   and ranked equal " 3".
- **The lowest three paragraphs are:**
  - Item No (10) " Enough budget is given to help implement the plans " 51.2%"   and ranked equal " 9".
  - Item No(11) " Certain programs are identified to help in the implementation process “51%"   and ranked equal " 10".
  - Item No (7)" There is a incentives system for workers to encourage them to implement the plans and reach the required targets”43%"   and ranked equal “11".

The results in table (5.15) denote the following facts:

The result in Table (5.15) shows that the approval toward domain four “implementation of the strategic plan for information security” is less than moderately (56.42) this implies that there is weak interest in government institutions to implement a strategic plan for information security, so the management in government institutions should be doubled efforts to motivate staff to implement information security strategic plans. The researcher attributed this result to the political and economic situation in Gaza, which leads to weaken the morale of the staff, and leads to the lack of adequate budgets for the implementation of and follow-up plans, In addition, some staff are convinced that the plans are ineffective.

In detail,

- The degree of approval of respondents ‘opinions towards “The institution has an operational plan to achieve annual objectives “is good (70.6). that implies that government institutions has good interesting about information security and try to achieve good level in security.
- The degree of approval of respondents ‘opinions towards “The procedures set in strategic plan are implemented by all employees each according to his/her

responsibilities” was moderately, this is evidence that there is no adequate monitoring, and the unwillingness of the staff to work.

- The degree of approval of respondents ‘opinions towards “The set plan is converted into programs, activities, and procedures, the identified activities are implemented on time, the activities are set in accordance with the identified objectives and purposes, taking into consideration the changing environmental conditions, the identified activities include all aspects specific to Information security, The institution has an effective administration, and leaders encouraging the employees to achieve the objectives, Enough budget is given to help implement the plans” is less than moderately (50-59), this is evidence that there is no adequate oversight, and the unwillingness of the staff to work. The main reason ,as the researcher believes, is the political and economic situation, which has a negative impact on the staff and on their performance
- The finding agreed with Abu_musa(2010) that the approval of respondents ‘opinions towards (The existence of policies, programs and activities private of information security)was less than moderately(57%). The agreement returns to the information security is relatively new issue, the respondents have no enough experience to deal with it strategically
- The finding disagreed with Sahli(2011) Where civil defense officers’ opinion in Saudi Arabia gave a high percentage of approval(80.9%) on " implementation the strategic plan for disaster damage reduction". The difference is due the respondents have enough experience in strategic management. Also disagreed with Dirawi(2014) where he did not address the process of implementation of the plan in his study.

5.3.2.5 Fifth Domain: Control and monitoring of the implementation of the ISSP:

Table (5.16)The respondents’ opinions towards the items of the fifth domain

#	Question	mean	Weight mean%	Value (t)	Sig	Rank
1	There is an effective performance evaluation system	5.860	58.6	5.25**	0.000	2
2	Performance and level of security are periodically evaluated according to specific criteria	5.800	58	5.06**	0.000	3
3	There is a mechanism for the periodic review of the Plan'sactivities	5.280	52.8	3.62**	0.000	9
4	Planning team periodically reviews strategic plans and programs	5.160	51.6	3.63**	0.000	10
5	There are monitoring and follow-up programs to make sure things are going as planned	5.520	55.2	5.04**	0.000	7
6	The institution uses external evaluation processes	4.500	45	2.25*	0.012	11

#	Question	mean	Weight mean%	Value (t)	Sig	Rank
7	Necessary measures are taken to ensure the progress of work in case of any change in the environment or any gaps between what was planned and what is executed	5.540	55.4	5.07**	0.000	6
8	The institution has an effective accountability system	5.520	55.2	4.38**	0.000	8
9	The institution follows official procedures for reporting vulnerabilities in the plan and suggestions to solve them	5.760	57.6	5.27**	0.0000	4
10	The institution uses security auditing	5.940	59.4	5.50**	0.000	1
11	There are matching process between the results of the strategic plan and objectives	5.600	56	4.95**	0.000	5
All items		5.498	54.98	4.55**	0.000	

The responses of the study sample toward fifth domain show the following results:

The mean of responses to all paragraphs in this domain (4.50-5.94) with weight mean (45%-59.4%). According to the gradient scale decimal, and the weight mean for fifth domain equal (54.98%) and the sig. (p-value) equals (0.000) less than (α = 0.05), which shows statistical significance and that the response level of this domain is less than the neutrality degree of (6). This indicates that the respondents disagreed with the domain *"Control and monitoring of the implementation of the ISSP"*

- **The top three paragraphs are:**
  - Item No. (10)" The institution uses security auditing "The institution uses security auditing " the weight mean equal " 59.4%" and ranked equal " 1"
  - Item No(1) " There is an effective performance evaluation system " " 58.6%" and ranked equal " 2"
  - Item No(2) " Performance and level of security are periodically evaluated according to specific criteria" the weight mean equal " 59%" and ranked equal " 3".

- **The lowest three paragraphs are:**
- Item No. (3)" There is a mechanism for the periodic review of the Plan's activities" the weight mean equal " 52.8%" and ranked equal " 1"
- Item No(4) " Planning team periodically reviews strategic plans and programs" the weight mean equal " 51.6%" and ranked equal " 2"
- Item No(6) "The institution uses external evaluation processes" the weight mean equal " 45%" and ranked equal " 3".

The results denote the following facts:

The above result shows that the approval toward domain five “Control and monitoring of the application of the Strategic Plan” was less than moderately (54.98) this implies that there is weak interest in government institutions to implement and control a strategic plan for information security, so the management in government institutions should double efforts in this point. The result is the interpretation of the results of the previous domain, where the weak monitoring and controlling lead to a lack of commitment to implementation of the plan.

In detail,

- The degree of approval of respondents ‘opinions towards” The institution uses security auditing” is moderately **(59.4)**
- The degree of approval of respondents ‘opinions towards (” There is an effective performance evaluation system", "the institution follows official procedures for reporting vulnerabilities in the plan and suggestions to solve them "."Performance and level of security are periodically evaluated according to specific criteria "," necessary measures are taken to ensure the progress of work in case of any change in the environment or any gaps between what was planned and what is executed" , "the institution has an effective accountability system, there are monitoring and follow-up programs to make sure things are going as planned”) is less than moderately(50-59)
- The degree of approval of respondents ‘opinions towards” The institution uses external evaluation processes” is weak. This process needs to budget, and this is not available at government institutions.
- This result from the perspective of the researcher is cumulative result, where the government institutions do not have a special team for information security of strategic planning, have weakness in process of environmental analysis, and the weakness of the drafting of the plan. All that leads to the inability of institutions to implement and control and follow-up of the plan and correct errors, also although aware of the administration and specialists of the importance of strategic planning for information security and its impact on the institution as a whole, but the political and economic circumstances do not help them. Therefore, the governmental institutions rely on the implementation of listed information security policies, without compliance within the strategic plan has limited time, activities and programs, to be followed up and evaluated.

➢ The finding agreed with Abu-musa(2010) that the approval of respondents ‘opinions towards (The existence an assessment system, the follow-up information security risks, and performance measurement and evaluation in Saudi Arabia’ Institutions)was less than moderately. The finding agreed with Altoom (2013) that the approval of respondents ‘opinions towards (The existence an assessment system, the follow-up information security policies in Palestinian universities) less than moderately (53.4%). That because the respondents have no enough experience in strategic planning for information security and how measure performance of it.

- The finding agreed with kazemi (2011) that the approval of respondents ‘opinions towards (The institution uses external evaluation processes) was weak, the researcher explains this point that the security issues, are very sensitivity, most organizations do not have a positive view about uses external advisors.
- The finding disagreed with Sahli (2011) where civil defense officers’ opinion in Saudi Arabia gave a high percentage (85.8%) of approval towards (The assessment and monitoring systems, and performance measurement and evaluation strategic plan for disaster damage reduction). The difference is due the experience of respondents.
- The finding disagreed with Tayh (2008) that the approval of respondents ‘opinions towards (The existence an assessment and monitoring systems in Palestinian tech companies)was good(73.1%).The difference is due the material and moral possibilities of Palestinian tech companies which raised the expertise of their staff in monitoring and evaluating information security.
- The study differ from Dirawi (2014) where he did not address the process of controlling and monitoring of the plan in his study.

5.3.2.6 Sixth Domain: The Level of Information Security.

Table (5.17)The respondents’ opinions towards the items of the sixth domain

#	Question	mean	Weight mean %	Value (t)	Sig	Rank
1	There is a classification guide for information, its assets, how to treat them, and how protect it from those who use it	5.860	58.6	5.13**	0.000	19
2	There is management ways to access information (identifying the privilege to gain access the information, how to access, and use audit records for any change)	6.600	66	7.48**	0.000	14
3	There is a continuous update for defensive programs to reduce the impact of malware	7.120	71.2	8.96**	0.000	2
4	There are policies that periodically guarantee the maintenance of information as a back-up process	7.880	78.8	12.22**	0.000	1
5	economic cost of the information security is low, compared with the cost of risk occurrence	7.000	70	9.24**	0.000	4

#	Question	mean	Weight mean %	Value (t)	Sig	Rank
6	There are clear policies to ensure the continuation of work at times of emergencies (power outage - the bombing – rain)	6.900	69	8.12**	0.000	6
7	Information is available, integrated and correct at all times	7.020	70.2	10.15**	0.000	3
8	There are strong policies to support networks ‘security, ensuring the absence of interference or breakthroughs.	6.740	67.4	8.17**	0.000	9
9	Employees comply with regulations and policies related to the preservation of data, destroying remnants of important information, and securing computer screens.	6.680	66.8	8.58**	0.000	11
10	There are clear procedures to limit devices' subversion operations	6.960	69.6	10.21**	0.000	5
11	Encryption mechanisms or similar procedures are taken to transfer data through the network to ensure their protection	6.580	65.8	7.47**	0.000	15
12	Information security policies are clarified according to the strategies at hand, according to each individual's responsibilities and under the limits of the information he/she deals with	6.420	64.2	7.70**	0.000	17
13	Information is available with the suitable quantity and accuracy	6.860	68.6	9.25**	0.000	8
14	There are procedures to protect the buildings and rooms containing devices and equipment	6.620	66.2	7.37**	0.000	13
15	There are particular procedures to deal with e-mail, installing programs, and web sites in the institution	6.880	68.8	8.82**	0.000	7
16	All the procedures followed in Information Security are subject to the generally accepted standards, and according to the specific areas	6.480	64.8	8.12**	0.000	16
17	There are mechanisms applied to follow up and estimate types and sizes of accidents and the damage caused	5.900	59	6.25**	0.000	18
18	There is a mechanism for the maintenance of devices and checking the output to make sure that the devices is working properly	6.680	66.8	9.13**	0.000	11
19	There is an Documentation process for breakdowns and breakthroughs, and how to act accordingly	6.700	67	8.80**	0.000	10
All items		6.727	67.27	8.48**	0.000	

The responses of the study sample toward sixth domain show the following results:

The mean of responses to all paragraphs in this domain (5.86-78.2) with weight mean (58.6%-78.2%) According to the gradient scale decimal, and the weight mean for sixth domain equal (67.27%) and the sig. (p-value) equals (0.000) less than (α = 0.05), which shows statistical significance and that the response level of this domain is greater than the neutrality degree of (6). This indicates that the respondents agree with “The *Level of Information Security”*

The top three paragraphs are:

- Item No. (4)" There are policies that periodically guarantee the maintenance of information as a back-up process " the weight mean equal " 78.8%" and ranked equal " 1"
- Item No(3) " There is a continuous update for defensive programmers to reduce the impact of malware “the weight mean equal " 71.2%" and ranked equal " 2"
- Item No(7) “Information is available, integrated and correct at all times” the weight mean equal "70.2%" and ranked equal " 3".

The lowest three paragraphs are:

- Item No. (12)" Information security policies are clarified according to the strategies at hand, according to each individual's responsibilities and under the limits of the information he/she deals with" the weight mean equal " 64.2%" and ranked equal " 17"
- Item No(17) " There are mechanisms applied to follow up and estimate types and sizes of accidents and the damage caused "the weight mean equal " 59%" and ranked equal " 18"
- Item No(1) “There is a classification guide for information, its assets, how to treat them, and how protect them from those who use it ”the weight mean equal " 58.6%" and ranked equal " 19".

The results above denote the following facts:

The approval toward domain sixth “level of information security” is more than moderately (67.27) this implies that there is interest in government institutions toward information security, and there are policies for that but they should be increase this interesting. The researcher attributed this result to what has been explained by a theoretical framework that there are special written information security policies for government institutions, but these policies are not well distributed among ministries and specialists, it also is not regulated under a plan according to the foundations of strategic planning.

In detail,

- The degree of approval of respondents ‘opinions towards” There are policies that periodically guarantee the maintenance of information as a back-up process” is high (78.8%) which confirms the existence of interest by government institutions to information security and its availability, the researcher' opinion is that this interest is due to the suffering of the Gaza Strip from the wars of electrical malfunction.
- The degree of approval of respondents ‘opinions towards” There is a continuous update for defensive programmers to reduce the impact of malware, There are clear procedures to limit devices' subversion operations, Information is available, integrated and correct at all times, There are clear policies to ensure the continuation of work at times of emergencies (power outage - the bombing – rain),economic cost of the information security is low, compared with the cost of risk occurrence “is good (69%-72%) This confirms the existence of interest by government institutions to information security field (Networks, Software, Physical and Environmental Security, Equipment) but it need to increase it. The reason of this attention is due to the occurrence of some breakthroughs, and some of the problems resulting from power cuts, in addition to some of the events of espionage.
- The degree of approval of respondents ‘opinions towards” There is management ways to access information (identifying the privilege to gain access the information, how to access, and use audit records for any change, There is a documentation process for breakdowns and breakthroughs, and how to act accordingly, There is a mechanism for the maintenance of devices and checking the output to make sure that the devices is working properly, There are mechanisms applied to follow up and estimate types and sizes of accidents and the damage caused)” is moderately(59-69%), that mean the government institutions need to redouble efforts in some fields of information security (personnel, buildings, organizational), and documenting events to take advantage of them later.
- The degree of approval of respondents ‘opinions towards” There is a classification guide for information, its assets, how to treat them, and how protect it from those who use it “is close to the moderately (58.6%). This paragraph explains why the results of the previous paragraphs, where despite the presence of written information security policies, but it is not, placed in a guide helps employees in their work.

➢ The finding agreed with Hassan(2013) that the approval of respondents ‘opinions towards (The effectiveness of information security in government institutions) was moderately(65%). That as the two studies in the same research population and convergent period of time.

- The finding agreed partially with Tom(2013)) that the approval of respondents ‘opinions towards items “There is a continuous update for defensive programs to reduce the impact of malware, There are strong policies to support networks ‘security, There are particular procedures to deal with e-mail, installing programs, and web sites in the institution ” was good in both. the researcher attributed this agreement that as the target groups in both studies are information technology professionals, the biggest focus will be in the field of networking and software.
- The finding disagreed with Tayh(2008) that the approval of respondents ‘opinions towards (level of information security in Palestinian tech companies)was good(73.1%). The difference is due the Palestinian tech companies have the ingredients allow it to keep pace with updates in the field of information security, and have Efficiencies help in applying the policies of information security.
- The finding disagreed with Dirawi (2014), Tom(2013), and Danaf (2013) that the approval of respondents ‘opinions towards (information security in Palestinian university) was good (73.74-76.76). According studies, the interest in information security has emerged in the Palestinian universities before its appearance in government institutions, this is due to the presence of experts in universities, in addition to the attempts of penetrate the university information system by some students. also that allocated budget in government institutions for the information security is weak due of the economic and political situation.
- The finding disagreed with abu-kmail (2011) that the approval of respondents ‘opinions towards(data Security procedures in Palestinian banks) was high (90%).
- The finding disagreed partially with Kazemi et al(2011)) that the approval of respondents ‘opinions towards item “Employees comply with regulations and policies related to the preservation of data, destroying remnants of important information, and securing computer screens. ” was high, This is because of the policies of accountability in the Iranian institutions, and the economic and political situation in Gaza that affect on employees' activity.

5.3.2.7 Components of Strategic planning for information security and the level of information security:

Table of all domain (5.18)

#	Domain	mean	Weight mean %	Value (t)	Sig	Rank
1	clarity of Information Security concept and awareness of importance of strategic planning for information security	6.706	67.06	6.82**	0.000	2
2	information security environment analysis	5.872	58.72	5.69**	0.000	4
3	The formulation of the strategic plan for information security	5.992	59.92	6.34**	0.000	3
4	Implementation of the strategic plan for information security	5.642	56.42	5.05**	0.000	5
5	Control and monitoring of the application of the Strategic Plan	5.498	54.98	4.55**	0.000	6
6	Level of information security	6.727	67.27	8.48**	0.000	1
All items		6.073	60.73	6.16**	0.000	

The responses of the study sample toward all domains show the following results:

The mean of responses to all paragraphs in this domain is between (5.498 _ 6.727) with weight mean (54.98%-67.27%) According to the gradient scale decimal. The weight mean equals (60.73%) and the sig. (p-value) equals (0.000) less than (α = 0.05), which shows statistical significance and that the response level is greater than the neutrality degree of (6). This indicates that the respondents agree with "*the ISSP "*

The result could be concluded

- "Level of information security" " the weight mean equal "67.27%" and ranked equal " 1".
- "The clarity of Information Security concept and awareness of importance of strategic planning for information security" the weight mean equal "67.06%" and ranked equal" 2".
- "The formulation of the strategic plan for information security" the weight mean equal " 59.92%" and ranked equal " 3"
- "information security environment analysis" the weight mean equal " 58.72%" and ranked equal " 4"
- "Implementation of the strategic plan for information security" the weight mean equal " 56.42%" and ranked equal " 5".
- "Control and monitoring of the application of the Strategic Plan" " the weight mean equal " 54.98%" and ranked equal " 6".

The weight mean of “strategic planning for information security” was (60.73%)

This result in table (5.18) shows that there is a moderate interest from government institutions towards strategic planning for information security. as it has been previously mentioned that there is a clear interest in information security and there are policies and mechanisms in the fields of information security, but it is not within an effective strategic plan based on the strategic planning components.

The researcher attributed all of these results mainly to the political and economic factors that reduce the physical and moral resources required in strategic planning.

And also affect the work of the staff in government institutions and their performance. As government institutions have good awareness of the importance of information security, they must pay attention to strategic planning for the security of information, and selected appropriate and effective alternatives according to available resources.

5.3.3 Hypothesis Testing

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

To clarify the impact, the researcher used linear regression model between the dependent variable and the independent variable.

Null Hypothesis: The strategic planning of information security dose not affects on the level of information security at the level of statistical significance at α ≤ 0.05 in the governmental institutions in Gaza.

Alternative Hypothesis: The strategic planning of information security affects positively on the level of information security at the level of statistical significance at α ≤ 0.05 through the point of view of managers and specialists in the governmental Institutions in Gaza.

If the sig. (p-value) was greater than the significance level at (α ≤ 0.05), then we could not reject the null hypothesis and this reveals that there does not exist a significant statistical correlation between the strategic planning of information security and the level of information security through the point of view of managers and specialists in the governmental Institutions in Gaza.. If the sig. (p-value) was less than or equaled the significance level at (α ≤ 0.05), then we should reject the null hypothesis and accept the alternative one. This confirms that the strategic planning of information security affects positively on the level of information security at the level of statistical significance at α ≤ 0.05 in the governmental Institutions in

Gaza. Indeed, the Pearson Correlation Coefficient test was applied for each field of information security strategic planning separately.

5.3.3.1 The First Hypothesis:

" *The clarity of the concepts awareness to importance of information security Strategic Planning affects positively on the level of information security at the level of statistical significance at α ≤ 0.05 through the perspective of managers and specialists in the governmental Institutions in Gaza*."

Correlations between variables

This hypothesis was tested by applying "Pearson correlation coefficient test" to figure out the relationship between the two variables.

Table (5.19)

Shows the number and value of the correlation coefficient and the level of significance

	NO	Pearson	Significance
clarity of the concepts awareness to importance of information security Strategic Planning	50	0.520	**0.000
Level of information security	50		

** Significant at 0.01 * Significant at 0.05 // not Significant

Through the table(5.19) is clear Significance=0.000 which is less than 0.05 and the Pearson _value =0.520 this implies there is a positive correlation statistically significant at the 0.05 level between the clarity of the concept of information security and awareness of its importance and the level of information security through point of view of managers and specialists in government institutions, that means the more clearly the concept of information security and awareness of its importance and the greater the level of information security through the perspective of managers and specialists.

Linear regression model:

To clarify the impact, the researcher used linear regression model between the dependent variable and the independent variable.

Table (5.20) shows the linear regression model for the first Hypothesis

Variables	Coefficient	T-test	Prob
Constant	2.646	2.665	0.010
clarity of the concepts and awareness of ISSP(D1)	0.609	4.223	0.000
R^2	0.520		
F_test	17.836		
Prob.	0.000		

Information security level = 2.646 + 0.609 * D1 (When D1 increases 10% then information security level increase 6.09%)

The model confirms that there is an impact of (the clarity of the concept of information security and awareness of the importance) on information security level,,the correlation relationship is a positive where the signal for the coefficient of the independent variable is positive, the level of significance of P -test less than 0.05 this means that the model is overall fit.

According to this result the first hypothesis “The clarity of the concepts awareness to importance of information security Strategic Planning affects positively on the level of information security at the level of statistical significance at $\alpha \leq 0.05$.” is accepted.

- The researcher attributed this result to the increasing awareness of the importance of strategic planning for information security will lead to work hard to develop effective and flexible plans, in addition will improve the behavior of employees in compliance with information security and related information processing policies which organized in the Information security plan.
- The result agreed with Veiga & Martins(2014) that improving the information security culture by training increase the level of information security in organization.
- This study agreed with Siam (2010) that there is positive correlation between awareness of management to the importance of strategic planning and the level of performance in Feminism enterprises in Gaza. This study agreed with Sahli (2011) that there is positive correlation between the awareness of civil defense officers in Saudi Arabia to the importance of strategic planning and the reduction of disaster damage. And agreed with Hall (2011) that there is positive correlation between the awareness to the importance of strategic planning for information security and performance in enterprises. The existence of an agreement between this study and other studies can be explained by the existence of a good category of respondents have approximately the same administrative thought because they have similar job or the same field of study.

5.3.3.2 The Second Hypothesis:

” *environment analysis affects positively on the level of Information security at the level of statistical significance $\alpha \leq 0.05$ through the perspective of managers and specialists in the governmental Institutions in Gaza*."

Correlations between variables

Table (5.21)

Shows the number and value of the correlation coefficient and the level of significance

	NO	P-coefficient	Sig
information security environment analysis	50	0.566	**0.000
Level of information security	50		

** Significant at 0.01 * Significant at 0.05 // not Significant

Through the table (5.21) is clear there is a positive correlation statistically significant at the 0.05 level between information security environment analysis and level of information security through the perspective of managers and specialists, where Significance=0.000 which is less than 0.05 and the Pearson _value =0.566 this implies the more information security environment analysis the greater the level of information security through the perspective of managers and specialists.

Linear regression model:

The researcher used simple linear regression model to clarify the impact of environment analysis on information security level.

Table (5.22) shows the linear regression model for the second Hypothesis

Variables	Coefficient	**t-Statistic**	Prob.
Constant	3.336	4.467	0.000
environment analysis(D2)	0.578	4.751	0.000
R	0.566		
F-test	22.576		
Prob.	0.000		

Information security level = 3.336 + 0.578 * D2 (When D2 rises 10% information security level will increase 5.78%

The model confirms that there is an impact of (environment analysis) on information security level, the correlation relationship is a positive where the signal for the coefficient of the independent variable is positive, the level of significance of P -test less than 0.05 this means that the model is overall fit.

According to this result the second hypothesis “environment analysis affects positively on the level of information security, at the level of statistical significance at α ≤ 0.05.” is accepted.

- This result is a natural point of view of the researcher as the internal and external environment will be the basis of a study to determine the adequate information to fill the gap of what exists and what is needed in the future and provide all the information to build a strong strategic plan for the information security that ensure the Confidentiality, Integrity and Availability of the information. This is consistent with the theoretical framework that previously reported by researcher, which confirms the effectiveness of environmental analysis required to achieve the goals of the strategic plans.

- This study agreed with Dirawi (2014) that there is positive correlation between environmental analysis of information systems in the Palestinian universities and information security. The reason for the agreement is that the respondents are familiar with the basics of strategic planning as well as goals of the information security ,and they have a common culture about the positive impact of the environment analysis on the effectiveness of the strategic plans to achieve the intended purpose. Also the study agreed with Shing(2010) the risk analysis a basic foundation to raise information security level.

5.3.3.3 Third Hypotheses

"The formulation of the strategic plan affects positively on the level of information security, at the level of statistical significance at $\alpha \leq 0.05$ through the perspective of managers and specialists in the governmental Institutions in Gaza"

Correlations between variables

This hypothesis was tested by applying "Pearson correlation coefficient test" to figure out the relationship between the two variables.

Table (5.23) shows the NO and value of the correlation coefficient and the level of significance

	NO	correlation coefficient	Sig
The formulation of the strategic plan for information security	50	0.540	0.000 **
Level of information security	50		

** Significant at 0.01 * Significant at 0.05 // not Significant

Through the previous table(5.23) is clear that there is a positive correlation statistically significant at the 0.05 level between information security strategic plan formulation and level of information security through the perspective of managers and specialists where Significance=0.000 which is less than 0.05 and the Pearson _value =0.540 this implies the more formulation of information security strategic plan the greater the level of information security through the perspective of managers and specialists.

Linear regression model:

The researcher used simple linear regression model to clarify the impact of the formulation of the strategic plan for information security on information security level.

Table (5.24) Shows the linear regression model for the third Hypothesis

Variables	Coefficient	**t-Statistic**	Prob
Constant	3.105	3.677	0.001
The formulation of the strategic plan for information security (D3)	0.605	4.450	0.000
R	0.540		
F-test	19.805		
Prob.	0.000		

Information security level = 3.105 + 0.605* D3 (When D3 increase 10% then Information security level increase 6.05%)

The model confirms that there is an impact of (The formulation of the strategic plan for information security) on information security level, the correlation relationship is a positive where the signal for the coefficient of the independent variable is positive, the level of significance of P -test less than 0.05 this means that the model is overall fit.

According to this result the third hypothesis "The formulation of the strategic plan affects positively on the level of information security, at the level of statistical significance at $\alpha \leq 0.05$" is accepted. The researcher considered this result is logical depending on the theoretical framework, which confirms that the formulation of clear mission, vision, objectives, and identifying appropriate alternatives and priorities leads to building a strong information security system, which commensurate with all the changes and raising the level of information security thereby the basic objectives (Confidentiality, Integrity and Availability of the data.) will be achieved.

This study agreed with Dirawi (2014) there is positive correlation between the drafting of the Strategic Plan (the mission and the vision and the goals and priorities of the crisis, and the formulation of policies) and information security. The researcher attributed the reason of agreement between studies, that the respondents have the same administrative culture (a good formulation of information security plan impact positively on the effectiveness of the strategic plan to achieve the intended purpose).

5.3.3.4 Fourth Hypotheses:

"*The implementation of the strategic plan affects positively on the level of information security, at the level of statistical significance at α ≤ 0.05 through the perspective of managers and specialists in the governmental institutions in Gaza***"**

Correlations between variables

This hypothesis was tested by applying "Pearson correlation coefficient test" to figure out the relationship between the two variables.

Table (5.25)

Shows the number and value of the correlation coefficient and the level of significance

	NO	Pearson coefficient	Significance
Implementation of the strategic plan for information security	50	0.632	**0.000
Level of information security	50		

** Significant at 0.01 * Significant at 0.05 // not Significant

Through the previous table(5.25) is clear that there is a positive correlation statistically significant at the 0.05 level between information security strategic plan Implementation and Level of information security through the perspective of managers and specialists where Significance=0.000 which is less than 0.05 and the Pearson _value =0.632 this implies The more Implementation of information security strategic plan the greater the level of information security through the perspective of managers and specialists.

Linear regression model:

The researcher used simple linear regression model to clarify the impact of the implementation of the strategic plan for information security on information security level.

Table (5.26) shows the linear regression model for the fourth Hypothesis

Variables	Coefficient	**t-Statistic**	Prob
Constant	3.103	4.602	0.000
The implementation of the strategic plan for information security (D4)	0.642	5.646	0.000
R	0.632		
F-test	31.879		
Prob	0.000		

Information security level = 3.103 + 0.642* D4 (When D4 increase 10% then Information security level increase 6.42%)

The Model confirms that there is an impact of (The implementation of the strategic plan for information security) on information security level, the correlation relationship is a positive, where the signal for the coefficient of the independent variable is positive, the level of significance of P -test less than 0.05 this means that the model is overall fit.

According to this result the fourth hypothesis “The Implementation of the strategic plan affects positively on the level of information security, at the level of statistical significance at $\alpha \leq 0.05$.” is accepted

The researcher explains this outcome depending on the theoretical framework that the presence of a strategic plan for the security of information which is no longer any benefits unless it is implemented, and through the development of measurable activities, including security policies according to international standards to achieve the desired goals.

The study agreed with Hall(2011) there is positive correlation between the implementation of strategic planning for the information security and the level of performance in the Washington University, the researcher considering that the level f information security is one of the performance indicators. this agreement is consistent with the theoretical framework and the respondents culture which confirms the implementation of strategic plan will help in raising the performance, and in my study the ISSP part of overall strategic plan of organization and the level of information security is performance level for this part.

5.3.3.5 Fifth Hypotheses:

“*The Control and monitoring of the application of the Strategic Plan affects positively on the level of information security, at the level of statistical significance at α ≤ 0.05 through the perspective of managers and specialists in the governmental Institutions in Gaza****”***

Correlations between variables

This hypothesis was tested by applying “Pearson correlation coefficient test” to figure out the relationship between the two variables.

Table (5.27)

Shows the number and value of the correlation coefficient and the level of significance

	NO	coefficient	Sign
Control and monitoring of the implementation of the Strategic Plan	**50**	**0.725**	****0.000**
Level of information security	50		

** Significant at 0.01 * Significant at 0.05 // not Significant

Through the previous table(5.27) is clear that there is a positive correlation statistically significant at the 0.05 level between control and monitoring of the information security strategic plan and Level of information security through the perspective of managers and specialists where Significance=0.000 which is less than 0.05, and the Pearson correlation coefficient =0.725 this implies The more control and monitoring of information security strategic plan the greater the level of information security through point of view of managers and specialists in government institutions.

Linear regression model:

The researcher used simple linear regression model to clarify the impact of the implementation of the strategic plan for information security on information security level.

Table (5.28) shows the linear regression model for the fifth Hypothesis

Variables	Coefficient	**t-Statistic**	Prob
Constant	2.842	5.040	0.001

Control and monitoring (D5)	0.707	7.289	0.000
R^2	0.725		
F-test	53.136		
Prob	0.000		

Information security level = 2.842 + 0.707* D5 (When D5 increases 10% then information security level increase 7.07%)

The model confirms that there is an impact of (Control and monitoring) on information security level; the correlation relationship is a positive, where the signal for the coefficient of the independent variable is positive, the level of significance of P-test less than 0.05 this means that the model is overall fit.

According to this result the fifth hypothesis “The Control and monitoring of the strategic plan affects positively on the level of information security, at the level of statistical significance at $\alpha \leq 0.05$.” is accepted.

The researcher attributed this result to the control and follow-up process is the key point to verify the implementation of the plan and to correct its course To ensure the raising of the level of information security to the extent that is difficult to penetrate, and ensures the achievement of key targets (the Confidentiality, Integrity and Availability of the information.) and thus ensures raise the level of performance in government institutions.

The Result of Main Hypotheses Test:

Correlations between variables

All **Hypotheses** indicated that “*There is a positive correlation statistically significant at the 0.05 level between the information security strategic planning and Level of information security through the perspective of managers and specialists in the governmental institutions in Gaza*“.

Multiple Regression Model

Calculating a coefficient of multiple determination (or multiple regression coefficient) and regression equation using two or more independent variables is termed multiple regression analysis (Saunders, et.al,2009).This analysis used to assess the strength of a cause-and-effect relationship between variables.

Table (5.29) shows the multiple regression models

Dependent Variable: Information Security level			
Variables	Coefficient	**t-Statistic**	Prob.

Constant	1.779	2.043	0.047
D1	0.210	1.359	0.181
D2	0.252	1.450	0.154
D3	0.217-	1.056-	0.297
D4	0.067-	0.310-	0.758
D5	0.680	4.125	0.000
Adj. R^2	0.546		
DW	1.031		
F-test	12.771		
Prob	0.000		

$$Y = 0.210*D1 +0.252*D2-0.217*D3-0.067*D4 +0.680*D5 +1.779$$

Y= information security level
D1 = clarity of the concepts and awareness of ISSP
D2= environment analysis
D3 = The formulation of the strategic plan for information security
D4= the implementation of the strategic plan for information security
D5= Control and monitoring

From the equation: When D1 rises 10% Y will increase 2.10%, D2 rises 10% Y will increase 2.52%, D3 rises 10% Y will decrease 2.17%, D4 rises 10% Y will decrease 0.67%, also when D5 rises 10% Y will increase 6.80%.

Table (5.29) shows the following:

- The p-value for F-test less than 0.05, so the model are overall fit, and the independent variables impact on the dependent variable.
- the Adj. R^2 =0.546 which means that 55% of the variation in the dependent variable are explained by the independent variables, and there are 45% other independent variables impact on the dependent variable.
- P-value for T-test for independent variables are greater than 0.05 except the last variable is less than 0.05,so there are other variables that affect the model more than these variables.
- The value of the DW- test is equal to 1.031 that means: the independent variables affect each other, that Causing weakening in the model.

The researcher considered this result is logical, and the model expresses the fact that the success of each process of strategic planning processes rely on the success process that preceded, thus, this dependence will adversely affect the main objective which is "information security level". In the event that any stage have not been implemented effectively.

However, the effect of each independent variable separately on the target was positive and it produced a suitable simple model, and this is agreed with the literatures of this study.

5.3.3.6 Sixth Hypothesis:

"*There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about Information security level attributed to their personal information*".

Sub-Hypothesis one: There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about Information security level through the perspective of managers and specialists in government institutions attributed to their qualification.

This hypothesis was tested by applying **Two _Independent sample T test**.

Table (5.30) Shows number, mean, T value, standard deviation, sign

Qualification	No	mean	standard deviation	T value	Significance
B.Sc	32	6.771	1.710	**0.220**	**//0.827**
Higher Studies	18	6.649	2.169		

** Significant at 0.01 * Significant at 0.05 // not Significant

Table (5.30) shows that the significance is greater than the significance level at (α ≤ 0.05) this result indicates that there are no differences among the respondents in their opinions attributed to the qualification level. According to this result could be rejected the sub-hypothesis "There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about Information security level through the perspective of managers and specialists In government institutions attributed to their qualification."

The researcher interpreted this result that the sample members have a good awareness of the importance of information security

This result agreed with the study of Hasan(2013) where he has found out that there were no differences among the respondents‘ opinions in government institutions attributed to their qualification. and agreed with the study of Derawi(2014), Altoom(2013) where they found out that there were no differences among the respondents‘ opinions towards their study fields attributed to qualification (Despite the different study population in their studies But they related to information security). This is because the scientific qualifications of the respondents are convergent related to information security and strategic planning.

Sub-Hypothesis two: There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about Information security level from the point of view of managers and specialists in government institutions in Gaza attributed to their specialization.

This hypothesis was tested by applying One-Way ANOVA Test.(F test)

Table (5.31) Shows the sum of the squares, the degree of freedom, the mean squares, test "F" and the level of significance

	Sum of Squares	Df	Mean Square	**F value**	**Significance**
Between Groups	16.267	3	5.422	1.614	.199 //
Within Groups	154.523	46	3.359		
Total	170.791	49			

** Significant at 0.01 * Significant at 0.05 // not Significant

Table (5.31) shows that the significance is greater than the significance level at (α ≤ 0.05), this result indicates that there are no differences among the respondents in their opinions over Information security level In government institutions attributed to specialization. According to this result the sub-hypothesis could be rejected ―There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions over the Information security level from the point of view of managers and specialists in government institutions attributed to their specialization.

Moreover, it can conclude that the study sample individuals have a correspondent opinion over the information security level regardless of the specialization, this is because the sample work is closely related to information security, therefore, they are fully aware of the seriousness of the information exposure for any damage, and the need for accurate and correct information to issue appropriate decisions.

This result agreed with the study of Hasan (2013) where he has found out that there were no differences among the respondents' opinions in government institutions attributed specialization. And agreed with Derawi (2014) where he has found out that there were no differences among the respondents' opinions about information security attributed specialization. This is because the specialization of the respondents in the both studies are convergent these are either in Business Administration or IT.

Sub-Hypothesis three

There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about information security level attributed to experience.

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

Table (5.32) Shows the sum of the squares, the degree of freedom, the mean squares, test "F" and the level of significance

	Sum of Squares	Df	Mean Square	**F value**	**Significance**
Between Groups	18.315	2	9.158	2.823	.070 //
Within Groups	152.475	47	3.244		
Total	170.791	49			

** Significant at 0.01 * Significant at 0.05 // not Significant

Table (5.32) shows that the significance is greater than the significance level at (α ≤ 0.05), this result indicates that there are no differences among the respondents in their opinions over Information security level In government institutions attributed to experience. According to this result the sub-hypothesis (There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions over the about Information security level through the perspective of managers and specialists in government institutions attributed to experience years) could be rejected.

This is because the majority of respondents have the same group for the years of experience, and that's where the information security is sensitive subject to all employees.

- This result agreed with the study of Dirawi(2014) where he has found out that there were no differences among the respondents‘ opinions attributed experience years.
- This result disagreed with the study of Hasan(2013) where he has found out that there were differences among the respondents‘ opinions in government institutions attributed experience years, and disagreed with Tom(2013) where he has found out that there were differences among the respondents‘ opinions about information security attributed experience years.

Sub-Hypothesis Four

“There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about the level of information security attributed to the governmental institution they belong to”.

This hypothesis was tested by applying **Two- Independent sample T test**.

Table (5.33)Shows number, mean, T value, standard deviation, sign

Governmental Institution	**No**	**mean**	**standard deviation**	**T value**	**Significance**
Ministry of Telecommunication and Information Technology	29	7.410	1.526	**3.339**	****0.002**
Interior and National Security Ministry	21	5.784	1.916		

** Significant at 0.01 * Significant at 0.05 // not Significant

Table(5.33) shows that the significance is less than the significance level at (α ≤ 0.05), this result indicates that there are differences among the respondents in their opinions over information security level in government institutions attributed to the governmental institution they belong to. It was in favor of the Communications Ministry. This is because the Ministry of Communications is gathering all the ministries which decide the information security policies to all ministries and government institutions.

According to this result the sub-hypothesis (There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about Information security level through the perspective of managers and specialists in government institutions attributed to the governmental Institution they belong to**)** is accepted

Sub-Hypothesis five

There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about information security level through the perspective of managers and specialists in government institutions attributed to age.

This hypothesis was tested by applying One-Way ANOVA Test to determine if there are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions

Table (5.34)Shows the sum of the squares, the degree of freedom, the mean squares, test "F" and the level of significance

	Sum of Squares	Df	Mean Square	**F value**	**Signi**
Between Groups	7.445	3	2.482	.699	.558 //
Within Groups	163.345	46	3.551		
Total	170.791	49			

** Significant at 0.01 * Significant at 0.05 // not Significant

Table (5.34) shows that the significance is greater than the significance level at (α ≤ 0.05), this result indicates that there are no differences among the respondents in their opinions over information security level in government institutions attributed to age. According to this result the sub-hypothesis “There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about Information security level the perspective of managers and specialists in government institutions attributed to age “ is rejected.

Moreover, the researcher can conclude that the study sample individuals have a same vision over the study fields with regard to their age, that the main reason as was mentioned that the issue of information security is an important issue that occupy the thought of anyone that deal with it.

- This result agreed with the study of Dirawi(2014),Tom(2013), Tayh(2008) where they found out that there were no differences among the respondents‘ opinions attributed to age.
- This result disagreed with the study of Hasan(2013) where he has found out that there were differences among the respondents‘ opinions in government institutions attributed to age. That due Hassan’s study includes a varying age groups and some of them over45, while the age groups in this study are similar and relatively small.

Sub-Hypothesis six: There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about the information security level attributed to their gender.

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

Table (5.35) Shows number, mean, T value, standard deviation, sign

Qualification	No	mean	standard deviation	T value	Significance
Male	40	6.650	1.876	**0.582**	**//0.563**
Female	10	7.037	1.896		

** Significant at 0.01 * Significant at 0.05 // not Significant

Table (5.35) shows that the significance is greater than the significance level (α ≤ 0.05). This result indicates that there are no differences among the respondents in their opinions over the information security level attributed to gender. According to this result the sub-hypothesis” .There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about the information security level attributed to their gender” is rejected

Researcher explained this result that the information security issue is difficult subject and all members of the sample at high capacity to deal with this topic,

- This result agreed with the study of Derawi(2014), Altoom(2013) and Hasan(2013) where they found out that there were no differences among the respondents‘ opinions towards their study fields attributed to gender.

Sub-Hypothesis seven: There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about Information security level through the perspective of managers and specialists in government institutions attributed to Job title.

This hypothesis was tested by applying One-Way ANOVA Test to determine if there are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions

Table (5.36) Shows the sum of the squares, the degree of freedom, the mean squares, test "F" and the level of significance

	Sum of Squares	Df	Mean Square	**F value**	**Significance**
Between Groups	25.395	5	5.079	1.537	.198 //
Within Groups	145.395	44	3.304		
Total	170.791	49			

** Significant at 0.01 * Significant at 0.05 // not Significant

Table (5.36) shows that the significance is greater than the significance level (α ≤ 0.05) This result indicates that there are no significant differences among the respondents in their opinions over the information security level attributed to Job title. According to this result the sub-hypothesis" There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about the information security level attributed to Job title" is rejected.

The researcher attributed this result that the study sample is divided into two parts, the first are information technology specialists and they are working within the job title relate with their specialization, and part of the managers who have limited their dealings with the security of information.

- This result agreed with the study of Derawi (2014), Altoom(2013) and where they found out that there were no differences among the respondents' opinions towards their study fields attributed to job title. This compatibility due to that all Job titles in all studies focus on one field which is the security of information.

Sub-Hypothesis eight: There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about the information security attributed to their main work field.

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

Table (5.37) Shows the sum of the squares, the degree of freedom, the mean squares, test "F" and the level of significance

	Sum of Squares	Df	Mean Square	**F value**	**Significance**
Between Groups	8.859	4	2.215	.615	.654 //
Within Groups	161.931	45	3.598		
Total	170.791	49			

** Significant at 0.01 * Significant at 0.05 // not Significant

Table (5.37) shows that the significance is greater than the significance level (α ≤ 0.05).This result indicates that there are no significant statistical differences among the respondents in their opinions over the information security level attributed to their main work field.

According to this result the sub-hypothesis —"There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about the information security level attributed to their main work field. " is rejected.

As it has been previously noted the work of all study samples is directly related to information security and its policies

- This result agreed with the study of Hasan(2013) where he has found out that there were no differences among the respondents' opinions in government institutions attributed to their main work field.

Sub-Hypothesis nine: There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about the information security attributed to Training in the field of strategic planning for information security.

This hypothesis was tested by applying **Two-independent samples T Test** to determine if there are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions over the study fields attributed to Training in the field of strategic planning for information security.

Table (5.38)Shows number, mean, T value, standard deviation, sign

Qualification	No	Mean	standard deviation	T value	Significance
There isn't	25	6.701	2.145	**0.099**	**//0.922**
1-3	25	6.754	1.585		

** Significant at 0.01 * Significant at 0.05 // not Significant

Table (5.38) shows that the significance is greater than the significance level (α ≤ 0.05). This result indicates that there are no differences among the respondents in their opinions over the information security level attributed to training in the field of strategic planning for information security.

According to this result the sub-hypothesis "There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about the information security level attributed to training in the field of strategic planning for information security" is rejected.

- This result agreed with the study of Dirawi(2014) where he has found out that there were no differences among the respondents' opinions in government institutions attributed to training.
- This result disagreed with the study of Danaf(2013) where he has found out that there were differences among the respondents' opinions in government institutions attributed to training.

Sub-Hypothesis Ten: There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about the information security attributed to Training in the field of information security.

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

Table (5.39) Shows the sum of the squares, the degree of freedom, the mean squares, test "F" and the level of significance

	Sum of Squares	Df	Mean Square	**F value**	**Significance**
Between Groups	0.778	2	.389	.107	.898 //
Within Groups	170.013	47	3.617		
Total	170.791	49			

** Significant at 0.01 * Significant at 0.05 // not Significant

Table (5.39) shows that the significance is greater than the significance level (α ≤ 0.05).This result indicated that there are no differences among the respondents in their opinions over the information security level attributed to training in the field of information security.

According to this result, the sub-hypothesis- ”There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about the information security level attributed to training in the field of information security” is rejected.

- This result agreed with the study of Dirawi (2014) where he has found out that there were no differences among the respondents ‘opinions in government institutions attributed to training.

- This result disagreed with the study of Danaf(2013) where he has found out that there were differences among the respondents‘ opinions in government institutions attributed to training.

According to this result of ten sub-hypotheses, the **Sixth Hypothesis:**
“There are significant statistical differences at level (α ≤ 0.05) among the respondents in their opinions about Information security level through the perspective of managers and specialists in government institutions attributed to their personal information” is rejected.

This result indicated that there are no differences among the respondents in their opinions over the information security level through the perspective of managers and specialists in government institutions attributed to their personal information.

CHAPTER SIX
CONCLUSIONS AND RECOMMENDATIONS

- Introduction
- Conclusions
- Correlations between the study fields
- Differences among the study respondents' opinions
- Recommendations
- Further Research

6.1 Introduction:

This chapter includes the most important conclusions which have addressed the impact of strategic planning of information security on the level of information security at the governmental institutions in Gaza through the perspective of managers and specialists. In addition, this chapter shows the proposed most important recommendations which may enhance information security in the Palestinian Governmental Institutions.

6.2 Conclusion:

The study revealed that the level of impact of information security strategic planning on the level of information security was approximately (60.73 %.). On the other hand, there were clear weaknesses in some fields of strategic planning like: Implementation of the strategic plan for information security and Control and monitoring of the application of the Strategic Plan.

The study revealed that there is a positive correlation statistically significant at the 0.05 level between the information security strategic planning and Level of information security through the perspective of managers and specialists in the governmental Institutions in Gaza.

The regression Model between dependent variable and independent variables was

(Y = 0.210*D1 +0.252*D2-0.217*D3-0.067*D4 +0.680*D5 +1.779), the model is fit but it is weak because the dependence between independent variables.

The study revealed that:

First domain:

- The clarity of Information Security concept and awareness of importance of strategic planning for information security in the governmental Institutions in Gaza was (67.06%) and ranked (2).

Second domain:

- The information security environment analysis in the governmental Institutions in Gaza was (58.72%) and ranked (4).

Third domain:

- The formulation of the strategic plan for information security in the governmental Institutions in Gaza was (59.92%) and ranked (3).

Fourth domain:

- Implementation of the strategic plan for information security in the governmental Institutions in Gaza was (56.42%) and ranked (5).

Fifth domain:

- The Control and monitoring of the application of the Strategic Plan in the governmental Institutions in Gaza was (54.98%) and ranked (6).

Sixth domain:

- The level of information Security in the governmental Institutions in Gaza was (67.27%) and ranked (1).

6.2.1 Correlations between the study fields:

First domain:

There is a positive correlation statistically significant at the 0.05 level between the clarity of Information Security concept and awareness of importance of strategic planning for information security and Level of information security through the perspective of managers and specialists in the governmental institutions in Gaza

That means:

The clarity of the concepts of information security and awareness to importance of information security strategic planning affects positively on the level of information security at the level of statistical significance at $\alpha \leq 0.05$ through the perspective of managers and specialists in the governmental institutions in Gaza.

Second domain:

There is a positive correlation statistically significant at the 0.05 levels between environment analysis of information security and Level of information security through the perspective of managers and specialists in the governmental institutions in Gaza.

That means:

Environment analysis affects positively on the level of information security, at the level of statistical significance at $\alpha \leq 0.05$ through the perspective of managers and specialists in the governmental institutions in Gaza

Third domain:

There is a positive correlation statistically significant at the 0.05 level between the formulation of the strategic plan for information security and level of information security through the perspective of managers and specialists in the governmental institutions in Gaza.

That means:

The formulation of the strategic plan covering all of the points of SWOT affects positively on the level of information security, at the level of statistical significance at $\alpha \leq$

0.05 through the perspective of managers and specialists in the governmental institutions in Gaza.

Fourth domain:

There is a positive correlation statistically significant at the 0.05 level between Implementation of the strategic plan for information security and Level of information security through the perspective of managers and specialists in the governmental institutions in Gaza.

That means:

Implementation of the strategic plan affects positively on the level of information security, at the level of statistical significance at $\alpha \leq 0.05$ through the perspective of managers and specialists in the governmental institutions in Gaza

Fifth domain:

There is a positive correlation statistically significant at the 0.05 level between Control and monitoring of the application of the strategic plan and level of information security through the perspective of managers and specialists in the governmental institutions in Gaza.

That means:

Control process on the strategic plan affects positively on the level of information security, at the level of statistical significance at $\alpha \leq 0.05$ through the perspective of managers and specialists in the governmental institutions in Gaza

6.2.2 Differences among the study respondents' opinions:

- There are no significant statistical differences at level ($\alpha \leq 0.05$) among the respondents in their opinions about the study fields attributed to experience, gender, age, work field,job title, level of qualification, specialization and training.
- There are significant statistical differences at level ($\alpha \leq 0.05$) among the respondents in their opinions about the study fields attributed to the governmental institutions belong to.

6.3 Recommendations:

Palestinian Government is advised to exert more efforts towards strategic planning for information security.

In detail

First domain:

- Palestinian Government is recommended to increase the awareness of information security.

- Palestinian Government is recommended to increase the awareness of strategic planning of information security.
- Palestinian Government is recommended to enhance training in fields of information security and strategic planning for it.

Second domain:

- Palestinian Government is advised to pay more attention to the process of internal and external environment analysis when prepared to information security strategic plan

Third domain:

- Palestinian Government is advised to exert more efforts towards the formulation of information security strategic plan.
- Palestinian Government is recommended to devote a special team with highly qualified for strategic planning of information security,

Fourth domain:

- Palestinian Government is advised to exert more efforts towards the implementation of information security strategic plan.
- Palestinian Government is advised to allocate suitable budget for strategic planning of information security
- Palestinian Government is recommended to use incentives system to encourage the staff to implement policies for information security.

Fifth domain:

- Palestinian Government is advised to exert more efforts towards the Control and monitoring of the implementation of the information security strategic plan.
- Palestinian Government is recommended to enhance the external evaluation processes of information security.

Sixth domain

- Palestinian Government is recommended to convert written information security policies to strategic plans.

Palestinian Government is recommended to join international conferences regarding the information security, to learn from other experiences worldwide

6.4 Future Researches

In the light of the previous findings, the researcher proposes the following research:

- The factors that have impacts on information security strategic planning
- Impact of external evaluation on information security
- Alignment between strategic planning for information security and strategic planning of the institution in government institutions
- The impact of information security to the competitive advantage strategically.

REFERANCES:

Books:

- Ashenden, D, (2008), "Information Security management: A human challenge?", Information Security Technical Report, Vol.13, No.4: 195-201.

- Anderson,K 2003,"The past and future of information systems" *Series Editors*

- Boltz. J(1999) "Informational Security Risk Assessment: Practices of Leading Organizations", GAO/AIMD-00-33.

- Bagad,V.S.(2008)Management Information Systems, 3rd Revised Edition, India:Technical Publication Pune.

- Bateman.Th & Snell.S(2010) "Management:leading & collaborating I Competitive world"

- David.F.R (2011),"Strategic Management Concepts and Cases",, Pearson Education, Inc, New Jersey.

- ENISA(2006) "How to raise information security awareness"

- Elsaid,I(2005)"Strategic Management: Concepts and practical cases" Al-Dar Al_Jamaaia for Printing and Publishing, Egypt.

- Gamble,J. Thompson Jr. &Peteraf,M. 2013 "Essentials of Strategic Management: The Quest for Competitive Advantage 3rd Edition, McGraw-Hill Education

- Galiby,S. & Amiry,T. (2008) "Business and Management" Dar El-Yazouri for publication, Amaan Jordan.

- Goneem,M. 2008 "Planning: the foundations and principles", Dar Al Safa For Printing, Publishing and Distribution, Amman, Jordan.

- Gheitas.J.M (2007) "Information security and national security ", Dar Al Nahda for printing, publishing and the distribution, Cairo: 842:00; 24 cm.

- George, D. & Mallery, P. (2006). SPSS for Windows step by step: A simple guide and reference. (5th ed.). Boston, MA: Allyn & Bacon.

- Hill,C. & Jones,G,(2012) Essentials of Strategic Management Third Edition, south-Western,USA

- Hamdan,Kh. & Idris,W. (2009)," Strategy and strategic planning contemporary approach", Dar El-Yazouri for publication, Amaan Jordan.

- Hansche,S, CISSP, Berti,J, & Hare,CH 2004 " Official (Isc)2 Guide to the Cissp Exam"

- IT GI (2006), Information Security Governance Guidance for Boards of Directors and Executive Management", 2nd Edition, Meadows, USA

- Laudon.K & Laudon.J,2012" management information system managng the digital firm ",(12th).

- Mintzberg,H (2002) " Strategy Safari: The complete guide through the wilds of strategic management " (2nd Edition) 2nd

- Mintzberg, H. Ahlstrand, B. & Lampel,J. 1998. Strategy Safari: A Guided Tour Through the Wilds of Strategic Management. New York, NY: The Free Press.

- Peltier TH.R,(2014), "Information Security Fundamentals ",2d ed, CRC Press Llc,New York.

- Piccol,G. (2013) "Management Information Systems",,5ed, McGraw-Hill Education

- Peltier.TH, Peltier.J & Blackley.J,(2005), "Information Security Fundamentals ", CRC Press Llc,New York.

- Posthumus, S. & Von Solms, R. (2004). "A framework for the governance of information security, *Computers & Security,* 23(8): 638-646.

- Pearce, Robinson (2001),"Strategic Management: Formulation, Implementaion, & control", 12th ed, Mcgraw Hill Higher Education,New York, **pp** 992.

- Pfeiffer,J.,Goodstein,L & Timothy Nolan,T, 1993," Applied Strategic Planning: How to Develop a Plan That Really Works"

- Rumelt, R.; Schendel,D. & David J. 1994. Fundamental Issues in Strategy: A Research Agenda. Boston: Harvard Business School Press.

- Rothaermel.F (2015)," Strategic Management ", 2d ed,McGraw-Hill Education, New York.

- Robbins,S.P & Coulter,M. (2009) "Management ", pearson international edition, Pearson Prentice Hall Inc, River New Jersey.

- Salmi, Alaa Abdel Razek (2008) Electronic administration,Dar Wael for publication,Jordan - Amman

- Stewart J, Chapple M. & Tittel,Ed. (2004)," Certified Information Systems Security Professional",3rd ed, Neil Edde,San Francisco, London.

- Stamp,M 2006 "Information Security Principles and Practice" Second Edition

- Sultan,I 2009," Management Information Systems - Systems Approach ",Dar aljamaaia, Egypt.

- Stalling,W 2008 "Computer Security: Principles and Practice" 3th

- Smerhorn, Jr.2013 " Introduction to Management", 12th Edition International Student Version.

- Thomas,L. 2005 "Capacity building for local NGOs A guidance manual for good practice", Catholic Institute for International Relations, London N1 7BJ, UK

- Thompson Jr.,Stricklad, III. & Gamble,M. 2008 “Crafting and Executing Strategy: Concepts and Cases “ 16 th Edition, The McGraw−Hill Companies

- Vallabhaneni, S. Rao (2008). ” Corporate Management, Governance, and Ethics Best Practices” 1th.

- Wheelen.Th & Hunger.D,(2012) ”Strategic Management and Business Policy,Toward Global Sustainability “, 13th ED, Pearson Education, Inc, New Jersey.

- Whitman.M & Mottord.H(2011) “ Information Security “,4th ed.

- Whitman.M & Mottord.H(2012) “management information system ”, 4th ed.

- Yassin,G 2010,”Essentials of Pronciples of MIS and IT ” Dar Elmanahj,, Amman, Jordan.

Papers and Article

- Abu-Musa,A (2010) "Information security governance in Saudi organizations: an empirical study", Information Management & Computer Security, Vol. 18 Iss: 4, pp.226 – 276.

- Al-Shakarchy,N. (2013)“Management in E-Government using Zero-Knowledge Authentication”, The First Scientific Conference the Collage of Sciences 2013,Security IRAQ) available at www.iasj.net/iasj?func=fulltext&aId=77109

- Bayuk J. (2009). *How to Write an Information Security Policy*. Retrieved on 04/06/2014 from http://www.csoonline.com/article/2124114/strategic-planning-erm/how-to-write-an-information-security-policy.html?page=2.

- Bharadwaj,M.(2011) “ Measuring The Value of Information Security”.
- Bowen, P., Hash, J., & Wilson, M. (2006). Information security handbook: A guide for managers., http://csrc.nist.gov/publication s/nistpubs/800-100/SP800- 100-Mar07-2007.pdf
- Das,S (2014) “Why Security is Needed ".

- Gupta & Sherman (2012) Determinants of Data Breache,s: A Categorization-Based Empirical Investigation, Journal of Applied Security Research, 7, 375-395.

- Handley, M. & Rescorla, E. (2006). Internet Denial of Service Considerations. Available at: http://tools.ietf.org/html/draft-iab-dos-05. (Date of access: October 31, 2006)

- Hall,J. Sarkani, Sh. & Mazzuchi,Th., (2011) "Impacts of organizational capabilities in information security", Information Management & Computer Security, Vol. 19 Iss: 3, pp.155 – 176

- 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.
- John P. Pironti(2010) “Developing an Information Security and RiskManagement Strategy”.,ISACA JOURNAL VOLUME 2, 2010.
- Jouini,M, Rabai,L, Aissa,A 2014,” Classification of security threats in information systems”
- Kazemi,M. and others(2012).”Evaluation of information security management system success factors: Case study of Municipal organization Iran “,African Journal of Business Management Vol. 6(14), pp. 4982-4989, 11 April, 2012, Available online at http://www.academicjournals.org/AJBM
- Muendo,D.(2014).Information Security Subcultures in Information Security Management: A Conceptual Framework, European Journal of Business and Management, Vol.6, No.38, 2014,ISSN 2222-1905 (Paper) ISSN 2222-2839 (Online) www.iiste.org
- Nickols,F., 2011,” Strategy, Strategic Planning, Strategic Thinking, Strategic Management “
- Neeuf,S 2000 “Introduction to strategic thinking”
- Ngoma,S(2012)Vulnerability of IT Infrastructures: Internal and External Threats
- Pufahl,J (2010),information security stratigic planning, Universty of Connecticut inforamtion security office.
- Ponemon Institute LLC, Research Report January 2012, “The Human Factor in Data Protection”.
- Rhee, H., Ryn, Y., & Kim, C. (2012). Unrealistic optimism on information security management. *Computer and Security, ELSEVIER, 31*, 221-232.
- Shapiro, J.(2003)"Strategic Planning Toolkit. CIVICUS: World Alliance for Citizen Participation", Retrieved from: http://www.civicus.org
- Stone,M(2009),:Security according to Buzan:A comprehensive security analysis”,Sciences Po – Paris, France,Columbia University, School of International and Public Affairs – New York, USA
- Stoneburner,G., Goguen1,A. & Feringa,A.(2002),Risk Management Guide forInformation Technology Systems,National Institute of Standards and Technology[online], Spec.Publ. 800-30, 54 pages Available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf
- Solms,B.V & Solms,R.V.(2005) “ From information security to business security”.

- Smith,D (2005), The Three Types of Strategy, Cima Strategic Services

- Saqallah,Z.(2012) " Strategic Planning Information System Security", Al Quds Open University (QOU) available at http://www.qou.edu/newsletter/security.jsp

- Scanlan,J. (2011):"Assessing the alignment of information security, strategic business, and strategic information system planning: A department of defense perspective", Publisher:BiblioScholar October 2012, 146 pages.

- Shing.M & Shing,Ch. 2010,"Information Security Risk Assessment Using Markov Models ",Electronic Commerce and Security (ISECS), ISECS.2010.97pp.403 – 406.

- Samaini,J. & Hazleton,A. 2008,"Information Security Management Programs: Organizational Assessment Lessons Learned and Best Practices Revealed" Privacy & Data Security Law Journal.

- Tapinos E., Dyson, R & Meadows, M. "The impact of performance measurement in strategic planning",international Journal of Productivity and Performance Management,ISSN: 1741-0401

- Veiga,A. & Martins,N 2014," Improving the information security culture through monitoring and implementation actions illustrated through a case study", Journal Computers & Security,Volume 49, March 2015, Pages 162–176

- Wentworth,R(2003) "Strategic planning for information security'

Thesis

- Abu_kmail,S (2011) "The development of internal controls to protect information prepared electronically in Palestinian banks". Master Thesis, Cairo University

- Altoom, R.J(2013) " Information Security and Communications Management in light of Networks Technology"Master Thesis,Islamic University

- Al-Saadi 2013, "Strategic planning and its relationship to corporate performance effectively, applied study on information technology companies in Oman

- Al Sahli,F (2011):"The Role of Strategic planning requirements in Diminishing Disasters Harms" Naif Arab University for Security Sciences, master's thesis in Management Science.

- Dirawi,K.(2014) "The Rrelationship between Strategic planning of Management Information Systems and Information Security in the Palestinian universities in Gaza Strip" Master Thesis in BMA,Alazher University.

- Eldanaf.A,2013 "The reality of management information systems security in the technical colleges in the Gaza Strip and ways of developing" Master Thesis,Islamic University

- Farra.M &Atallah.S. (2006). Strategic planning in construction companies in the Gaza Strip. Journal of Studies and Research Nagaria - Zagazig University 0.2006.

- Hassan, A. (2013): "Information Security Management for Strategic and Effective Implementation of E-Management In The Governmental Institutions In Gaza" Master Thesis,Islamic University.

- Jones,R 2002," Fundamentals of Strategic and Tactical Business Planning " MAST Thesis, Kansas State University

- Kazemi.M, Khajouei.H and Nasrabadi "Evaluation of information security management system success factors: Case study of Municipal organization (Iran. 28 November, 2011)

- POKU,D.K(2012) "The Effect of strategic planniing on the performance and operation of the agricultural devlopment bank", Master Thesis,Kwame Nkrumah University.

- Siam.A(2010)"Application of Strategic Planning and its Relationship with Performance of on Governmental Organization in the Gaza Strip"Master Thesis,Alazher University.

- Tayh,A. 2008:"Effectiveness of Information Security Management at the Palestinian Information Technology Companies",Master Thesis,Islamic University

- 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

-

Internet Websites

- Strategic Planning,Managing Strategically. http://www.twc.state.tx.us/boards/board_planstrat_planning.pdf
- http://searchdatamanagement.techtarget.com/feature/Information-security-A-strategic-approach (5-2015)
- http://alwatan.kuwait.tt/articledetails.aspx?Id=211762&YearQuarter=20123 (12-2014)
- http://en.wikipedia.org/wiki/Zachman_Framework (12-2014)
- http://www.tdwl.net/vb/showthread.php?t=28997 (2-2015)

APPENDIXS

APPENDIX (A) Questionnaire Arbitrators

No.	Name	Describtion
1	Dr. Samer safi	IUG - Faculty Of Commerce
2	Dr. Khaled Dehliz	IUG - Faculty Of Commerce
3	Dr. Wael Daya	IUG - Faculty Of Commerce
4	Dr. Sami Abu ross	IUG - Faculty Of Commerce
5	Dr. Yousef Baher	IUG - Faculty Of Commerce
6	Dr. Yousef Ashor	IUG - Faculty Of Commerce
7	Dr. Mohamed Fares	Al-Azhar University - Faculty Of Commerce
8	Dr. Yousef Abu-Shaaban	Al-Azhar University – IT
9	Dr. Alaa Hales	IUG- IT

APPENDIX (B) Arabic Questionnaire

الجامعة الإسلامية

عمادة الدراسات العليا

كلية التجارة

قسم إدارة الاعمال

الموضوع :استبانة

اخى الفاضل /اختى الفاضلة,,,

تقوم الباحثة بإجراء دراسة للحصول على على درجة الماجستير في إدارة الأعمال من الجامعة الإسلامية ، **بعنوان: "اثر التخطيط الاستراتيجي لامن المعلومات على مستوى امن المعلومات من وجهة نظر المدراء والمختصين فى المؤسسات الحكومية"**

و تمثل هذه الاستبانة أحد الجوانب المهمة للبحث بهدف التعرف على اراء المدراء والمختصين بالتخطيط الاستراتيجي لامن المعلومات من مدراء عامين ومدراء تكنولوجيا المعلومات ونظم المعلومات الإدارية ومدراء امن المعلومات ومساعديهم ومبرمجين ومهندسين وكل من له صلة بامن المعلومات, والتخطيط الاستراتيجي لامن المعلومات وعليه تم تصميم هذا الاستبيان لجمع البيانات اللازمة للدراسة.

فيرجى التكرم بمساعدة الباحثة في تعبئة الاستبيان بشكل موضوعي, وان الباحثة تبدي بالغ الشكر والتقدير لرحابة صدركم وتعاونكم في إتمام هذا البحث, كما تؤكد ان المعلومات التي سيتم الحصول عليها لن تستخدم الا لغرض البحث العلمي.

وتقبلوا فائق الاحترام والتقدير

الباحثة

مجدولين أبو شعير

المؤسسة:

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

1. المؤهل العلمي.

□دبلوم فاقل □بكالوريوس □ دراسات عليا

2. التخصص.

□هندسة حاسوب □ تكنولوجيا معلومات

□ إدارة أعمال □ غير ذلك (الرجاء التحديد....................)

3. العمر.

□أقل من 30 سنة □ من30-اقل من 40 □ 40-اقل من 50 □50 فاكثر

4. الجنس.

□ذكر □ أنثى

5. المسمى الوظيفي(اختر إجابة واحدة فقط من فضلك).

□مدير عام □ مدير دائرة □ رئيس قسم □مهندس □ مبرمج

□مدخل بيانات □غير ذلك (الرجاء التحديد.......................)

6. سنوات الخدمة

□ اقل من 5 سنوات □من 5 –اقل من 10 □ 10 سنوات فاكثر

7. المجال الرئيسي لطبيعة العمل.

□إدارة المؤسسة ورسم الخطط والسياسات والاستراتيجيات □ تطوير التطبيقات البرمجية

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

□غير ذلك (الرجاء التحديد.......................)

8. عدد الدورات بالتخطيط الاستراتيجي لأمن المعلومات

لا يوجد □1-3 □4-6 □7 فاكثر

9. عدد الدورات بأمن المعلومات بشكل عام

□ لا يوجد □1-3 □4-6 □7 فاكثر

القسم الثاني: محاور الدراسة (مكونات التخطيط الاستراتيجي لامن المعلومات ومستوى امن المعلومات). ضع الدرجة المناسبة من 1 الى 10

المحور الأول: وضوح مفهوم امن المعلومات والوعي لأهميته

م	السؤال	من 1- 10
1	يوجد وعي لدى الادارة العليا ان امن المعلومات هو جزء من امن المؤسسة	
2	لدى الادارة وعي وقناعة ان التخطيط الاستراتيجي لامن المعلومات جزء اساسي من التخطيط الاستراتيجي للمؤسسة باكملها	
3	يوجد قناعة لدى الإدارة ان أي انتهاك للمعلومات واي خلل بامنها سيؤدي الى تعطيل لاهداف المؤسسة بشكل عام	
4	يوجد فريق خاص للتخطيط الاستراتيجي لامن المعلومات مكون من الإدارة والمختصين بتكنولوجيا المعلومات	
5	يوجد وعي لدى المدراء والمختصين بنظم المعلومات ان التخطيط الاستراتيجي يزيد الثقة بين العاملين	
6	يمتلك المختصون بامن المعلومات فهم واضح أن مشاكل امن المعلومات لابد من حلها استراتيجيا وليس فنيا وتقنيا فحسب.	
7	يوجد فهم كامل ان امن المعلومات لايقتصر فقط على امن الحاسوب انه يتضمن امن الافراد وامن المعدات والمباني والبيانات وهذا كله يحتاج لخطط تنفيذية وسياسات لحمايته	
8	هناك وعي ان التخطيط الاستراتيجي يخفض التكلفة الاقتصادية	
9	هناك وعي ان التخطيط الاستراتيجي يضمن استغلال جيد للقدرات والموارد والفرص الخارجية ويسهم بالقضاء على نقاط الضعف	
10	يوجد برنامج تدريبي خاص لزيادة الوعي لأهمية التخطيط الاستراتيجي لامن المعلومات	

المحور الثاني: تحليل البيئة الداخلية والخارجية لامن المعلومات

م	السؤال	من 1- 10
1	يعتبر تحليل البيئة الداخلية والخارجية ركيزة أساسية للتخطيط الاستراتيجي لأمن المعلومات	
2	يوجد فريق متخصص لتحليل البيئة المعلوماتية الداخلي والخارجية	
3	يتم استخدام أدوات متعددة بعملية التحليل للوصول لادق النتائج	
4	يتم من خلال عملية التحليل تصنيف المعلومات والتركيز على المعلومات الأساسية	
5	يتم تحديد مصادر القوة الخاصة بامن المعلومات بموضوعية للعمل على توظيفها لدى المؤسسة	
6	يتم خلال التحليل البيئي تحديد التهديدات الداخلية والخارجية بموضوعية	
7	يتم تحديد احتمالية حدوث أي انتهاك ناتج عن التهديدات بمصداقية	
8	يتم تحديد شدة المخاطر الناتجة عن أي تهديد (من معدات معطلة – بشري او كوارث طبيعية) بفاعلية	
9	يؤثر ضعف او قوة الموارد البشرية والمالية والهيكل التنظيمي عند التحليل البيئي لامن المعلومات	
10	يتم الاخذ بعين الاعتبار جميع الجوانب السياسية والاقتصادية والاجتماعية والقانونية عند القيام بالتحليل البيئي لامن المعلومات في الهيئة	

11	يتم تحديد الموارد والمميزات اللازمة للنجاح والعمل على تطويرها.	
12	يوجد نظام للمعلومات يساعد في الحصول على المعلومات عن البيئة الخارجية والداخلية.	

المحور الثالث:صياغة الخطة الاستراتيجة لامن المعلومات

م	السؤال	من 1- 10
1	يوجد روؤية واضحة محددة بزمن معين لتحقيقها	
2	تعكس الرؤية الاستراتيجية لامن المعلومات ارتفاع مستوى الامن المعلوماتي	
3	يوجد في المؤسسة رسالة واضحة لامن المعلومات يمكن تحويلها لخطط وسياسات	
4	يتم وضع الأهداف العامة (الغايات) لأمن المعلومات على أساس نتائج التحليل البيئي	
5	ترتبط الرسالة والأهداف العامة لأمن المعلومات مع رسالة نظم المعلومات الإدارية لتدعم وتتكامل مع رسالة وثقافة المؤسسة لتحقيق الأهداف العامة	
6	توضع الخطة الاستراتيجة لامن المعلومات لتحقق توافر وتكامل وصحة المعلومة للجهات المصرح لها وبالوقت المناسب	
7	تتضمن الخطة الاستراتيجية لامن المعلومات تحديد المسؤوليات والواجبات لكافة العاملين	
8	يتم تحديد الموارد المطلوبة لتنفيذ الخطة بموضوعية	
9	يتم صياغة االخطة الاستراتيجية لامن المعلومات لتكون شاملة لكافة مكونات امن المعلومات	
10	يتم صياغة الخطة الاستراتيجية لامن المعلومات تبعا للمعايير الدولية	
11	يتم وضع خطط بديلة للتجاوب مع التغيرات البيئية المحتملة	
12	اي تغير في استراتيجية المؤسسة يتبعها تغير في سياسة امن المعلومات	
13	تتسم سياسات امن المعلومات بالوضوح وسهولة الفهم و المرونة في التعامل مع كافة المتطلبات	
14	تتم المقارنة بين البدائل الاستراتيجية وتبني الأفضل من حيث التكلفة والموارد المتاحة وتحقيق الأهداف	
15	تتم مشاركة كافة المختصون بتكنولوجيا المعلومات وكل من له علاقة بأمن المعلومات مع الإدارة في صياغة الخطة الإستراتيجية.	

المحور الرابع: تنفيذ للخطة الاستراتيجة لامن المعلومات

م	السؤال	من 1- 10
1	يتم تحويل الخطة الموضوعة لبرامج وانشطة واجراءات ببساطة ودون تعقيد	
2	يوجد خطط تنفيذية سنوية واضحة ومحددة خاصة بمستوى امن المعلومات لتحقيق الاهداف المطلوبة	
3	يتوفر لدى المؤسسة خطة تشغيلية لتحقيق الأهداف السنوية	
4	يتم تنفيذالاجراءات الموضوعة بالخطة الاستراتيجية من قبل الموظفين كل حسب مسؤولياته	
5	يتم تنفيذ الأنشطة المحددة بالوقت المحدد لها	
6	يتم وضع أنشطة حسب الأهداف والغايات المحددة مع مراعاة الظروف البيئية المتغيرة	
7	يوجد نظام حوافز للعاملين لتشجيعهم على تنفيذ الخطط و الوصول للاهداف المطلوبة	
8	الأنشطة المحددة تشمل كافة الجوانب الخاصة بامن المعلومات (افراد و معدات وشبكات..)	
9	يوجد بالمؤسسة ادارة فعالة وقيادات تعمل على تحفيز الموظفين لتنفيذ الأنشطة وتحقيق الأهداف	
10	يتم وضع موازنات كافية تساعد لتفيذ الخطط	

11	يتم تحديد برامج تساعد في عملية التنفيذ	

المحور الخامس: التحكم والمراقبة لتطبيق الخطة الاستراتيجية

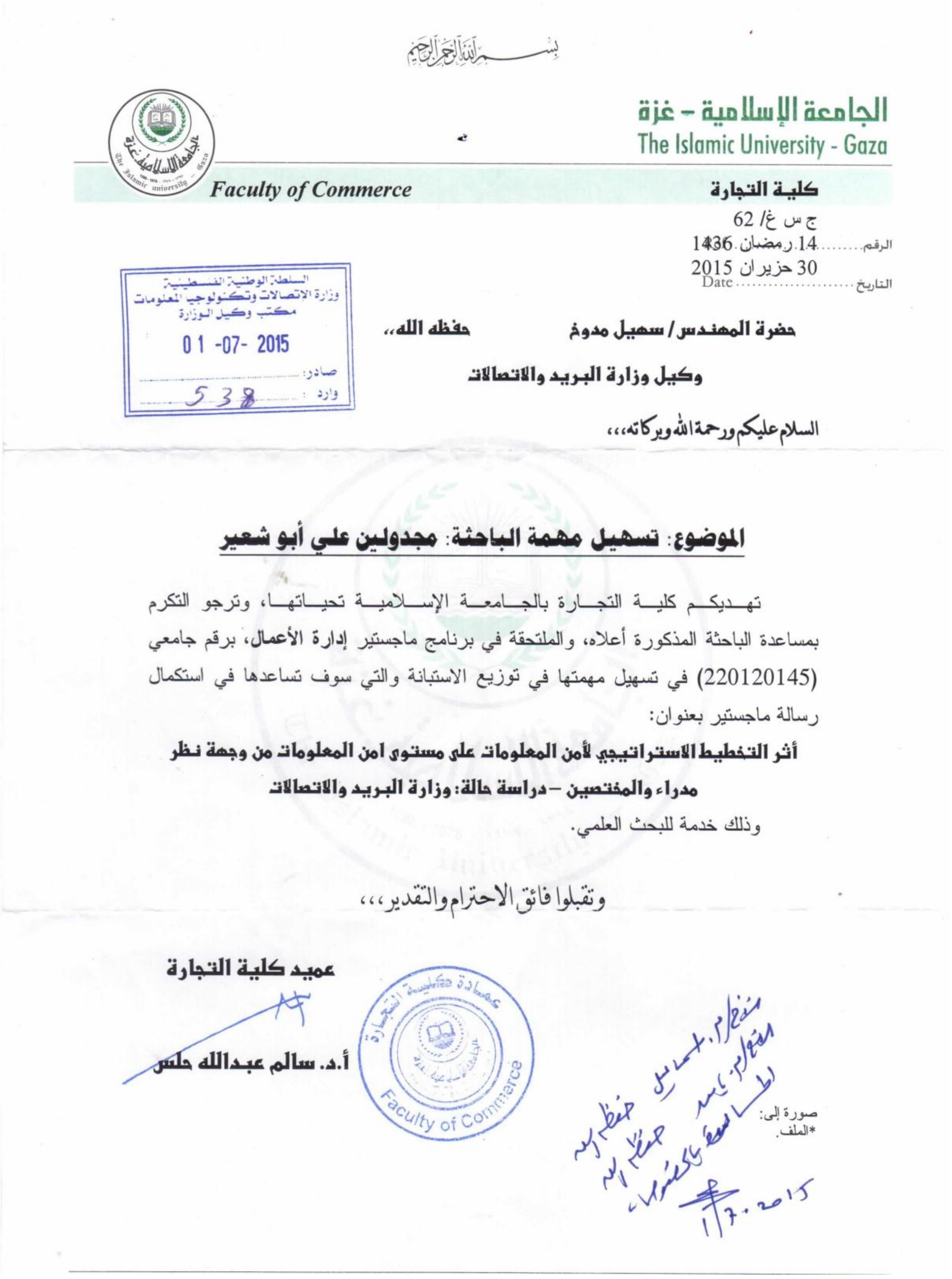
م	السؤال	من 1- 10
1	يوجد نظام فعال لتقيم الأداء	
2	يتم تقيم الأداء ومستوى الامن بشكل دوري وحسب معايير محددة	
3	يوجد الية مراجعة دورية للانشطة المحددة بالخطة	
4	يقوم فريق التخطيط بمراجعة الخطط الإستراتيجية والبرامج بشكل دوري	
5	يوجد برامج مراقبة ومتابعة للتاكد من سير الأمور كما تم التخطيط لها	
6	تستعين المؤسسة بعمليات التقيم الخارجي	
7	يتم اتخاذ الإجراءات اللازمة لضمان سير العمل في حال وجود أي تغير في البيئة او وجودات فجوات بين ما خطط له وما يتم تنفيذه	
8	يوجد في المؤسسة نظام مسألة فعال	
9	تتبع المؤسسة إجراءات رسمية لرفع التقارير بمواطن الضعف في الخطة واقتراحات حلها	
10	تستخدم المؤسسة ادوات التدقيق الامني (security auditing)	
11	تعمل المؤسسة على مطابقة نتائج الخطة الاستراتيجية بالاهداف المرجوة	

المحور السادس:مستوى امن المعلومات

م	السؤال	من 1- 10
1	يوجد دليل لتصنيف المعلومات والأصول المتعلقة بها وكيفية التعامل معها وحمايتها ومن مستخدمي هذا الأصل.	
2	يوجد إدارة لطرق الوصول للمعلومات (تحديد الصلاحيات للوصول للمعلومات وكيفية الوصول واستخدام سجلات التدقيق لاي تغيرات)	
3	يوجد تحديث مستمر للبرامج الدفاعية لتخفيض تاثير البرامج الضارة	
4	يوجد سياسات تضمن عدم فقدان للمعلومات كعملية نسخ احتياطي بشكل دوري	
5	تعتبر التكلفة الاقتصادية لامن المعلومات منخفضة بما يتناسب مع تكلفة تحقق الخطر.	
6	هناك سياسات واضحة لضمان سير العمل في حالات الطوارئ (انقطاع الكهرباء – القصف – الامطار)	
7	تتسم المعلومات انها متوافرة ومتكاملة وصحيحة بكل الاوقات	
8	يوجد سياسات قوية لدعم امن الشبكات مما يضمن عدم وجود اختراقات او تشويش.	
9	يمتثل الموظفين للوائح والسياسات الخاصة بحفظ البيانات و اتلاف مخلفات المعلومات الهامة وتامين شاشات الحاسوب	
10	هناك اجرءات واضحة للحد من عمليات تخريب الاجهزة.	
11	يتم استخدام اليات تشفير او إجراءات مشابهة لنقل البيانات عبر الشبكة لضمان حمايتها	
12	يتم توضيح سياسات امن المعلومات حسب الاستراتيجيات الموضوعة وكل حسب مسؤولياته وبحدود المعلومات التي يتعامل معها	

13	تعتبر المعلومات متوافرة بالكمية والدقة المناسبين	
14	هناك اجراءات لحماية المباني والغرف التي يوجد فيها الأجهزة والمعدات	
15	هناك اجراءت خاصة للتعامل مع البريد الالكتروني وتنصيب البرامج ومواقع الانترنت بالمؤسسة	
16	كافة الإجراءات المتبعة في امن المعلومات تخضع لمعايير المتعارف عليها وحسب المجالات المحددة	
17	يوجد اليات مطبقة تمكن من متابعة وتقدير أنواع واحجام الحوادث والتلف الذي تحدثه	
18	يوجد الية صيانة للأجهزة وفحص للمخرجات للتاكد من صلاحية الأجهزة	
19	يوجد عملية توثيق للاعطال او الاختراقات الحادثة وكيفة التصرف معها	

APPENDIX (C) Correspondence addressed to the ministries



بسم الله الرحمن الرحيم

الجامعة الإسلامية – غزة
The Islamic University - Gaza

Faculty of Commerce — كلية التجارة

الرقم: ج س غ/ 62
14 رمضان 1436
التاريخ Date: 30 حزيران 2015

حضرة المهندس/ سهيل مدوخ حفظه الله،،

وكيل وزارة البريد والاتصالات

السلام عليكم ورحمة الله وبركاته،،،

الموضوع: تسهيل مهمة الباحثة: مجدولين علي أبو شعير

تهديكم كلية التجارة بالجامعة الإسلامية تحياتها، وترجو التكرم بمساعدة الباحثة المذكورة أعلاه، والملتحقة في برنامج ماجستير **إدارة الأعمال**، برقم جامعي (220120145) في تسهيل مهمتها في توزيع الاستبانة والتي سوف تساعدها في استكمال رسالة ماجستير بعنوان:

أثر التخطيط الاستراتيجي لأمن المعلومات على مستوى امن المعلومات من وجهة نظر مدراء والمختصين – دراسة حالة: وزارة البريد والاتصالات

وذلك خدمة للبحث العلمي.

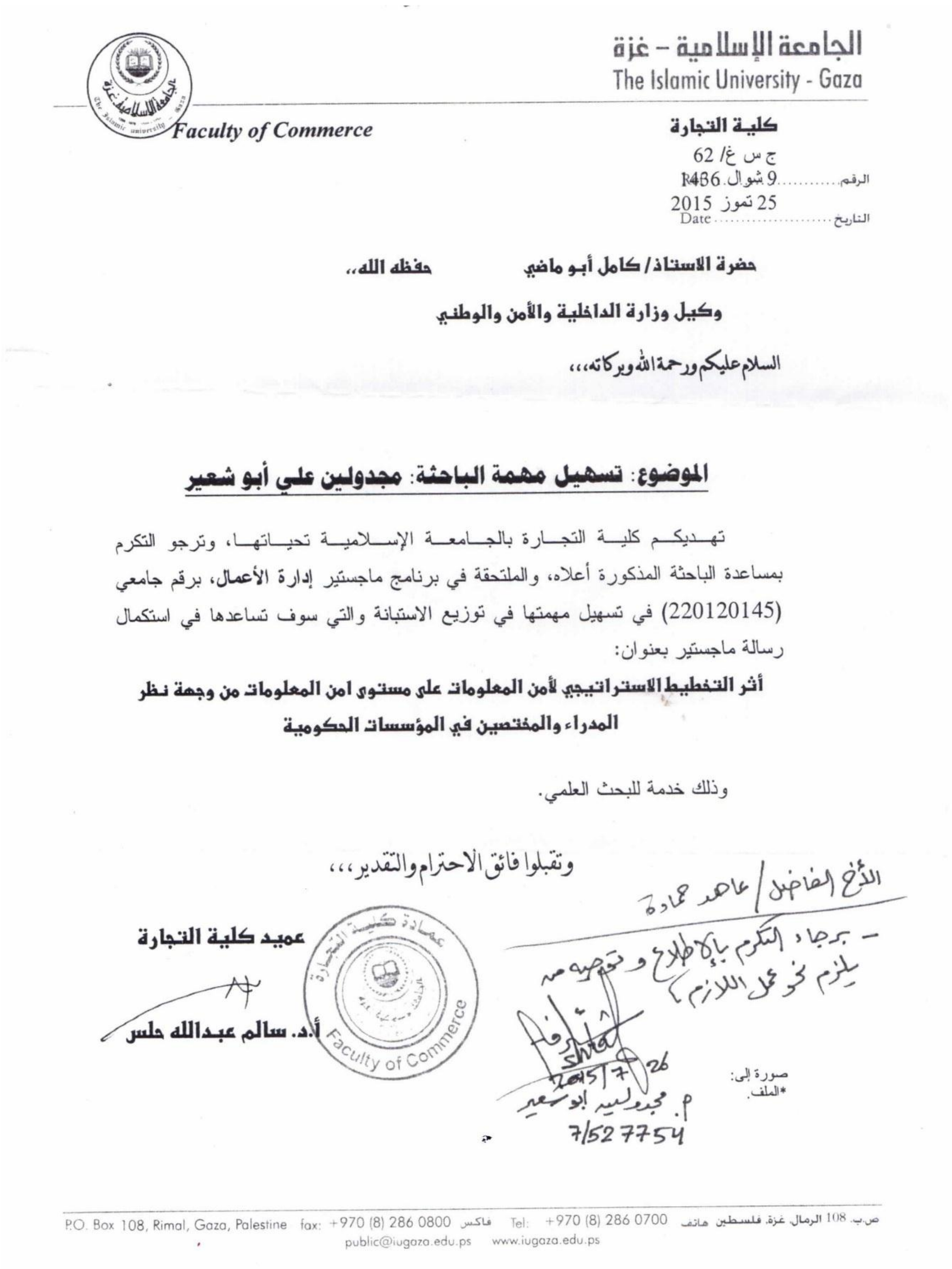
وتقبلوا فائق الاحترام والتقدير،،،

عميد كلية التجارة

أ.د. سالم عبدالله حلس

صورة إلى:
*الملف.

الأخ/م. اسماعيل حفظه الله
الأخ/م. ماجد حفظه الله
لطفاً للمساعدة مشكورين،
1/7.2015



الجامعة الإسلامية – غزة
The Islamic University - Gaza

Faculty of Commerce

كليـة التجارة

ج س غ/ 62
الرقم 9 شوال 1436
25 تموز 2015
التاريخ Date

حضرة الاستاذ/ كامل أبـو ماضي حفظه الله،،

وكيل وزارة الداخلية والأمن والوطني

السلام عليكم ورحمة الله وبركاته،،،

الموضوع: تسهيل مهمة الباحثة: مجدولين علي أبو شعير

تهديكم كلية التجارة بالجامعة الإسلامية تحياتها، وترجو التكرم بمساعدة الباحثة المذكورة أعلاه، والملتحقة في برنامج ماجستير **إدارة الأعمال**، برقم جامعي (220120145) في تسهيل مهمتها في توزيع الاستبانة والتي سوف تساعدها في استكمال رسالة ماجستير بعنوان:

أثر التخطيط الاستراتيجي لأمن المعلومات على مستوى امن المعلومات من وجهة نظر المدراء والمختصين في المؤسسات الحكومية

وذلك خدمة للبحث العلمي.

وتقبلوا فائق الاحترام والتقدير،،،

الأخ الفاضل/ عاهد حمادة

- برجاء التكرم بالإطلاع وتوجيه من يلزم نحو عمل اللازم،

2015/7/26

م. مجدولين ابو شعير
7/527754

عميد كلية التجارة

أ.د. سالم عبدالله حلس

عمادة كلية التجارة
Faculty of Commerce

صورة إلى:
*الملف.

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