

An-Najah National University
Faculty of Graduate Studies

**Information Security Management in
Palestinian Banking**

By
Abdellateef Lutfi Muhsen

Supervisor
Dr. Fady Draid

**This Thesis is submitted in Partial Fulfillment of the Requirements for
the Degree of Master of Science in Engineering Management, Faculty
of Graduate Studies, An-Najah National University, Nablus, Palestine.**


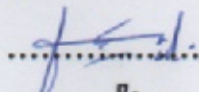
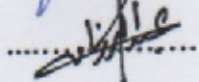
2014

**Information Security Management
in Palestinian Banking**

By

Abdellateef Lutfi Muhsen

This thesis was defended successfully on 15/6/2014, and approved by:

<u>Defense Committee Members</u>		<u>Signature</u>
Dr. Fady Draid	(Supervisor)	
Dr. Osama Marie	(External Examiner)	
Dr. Abdel-Razzak Natsheh	(Internal Examiner)	

Dedication

In this wonderful opportunity, I would like sincerely to express my deepest thanks and gratitude to all my beloved Family members and surroundings, and to dedicate this work especially to:

- ✓ My dear parents, who have given me the drive and discipline to tackle any task with enthusiasm and determination.
- ✓ My dear father-in-law and mother-in-law, who have been my constant source of inspiration.
- ✓ Dear wife for her understanding, patience and continuous support. Without her love and support this research would not have been made possible.
- ✓ My precious Kids “Lamar, Lutfi, Yazan” whom their presence in my life motivates me always to strive for the best.
- ✓ Treasured Brothers and Sisters “Hanan, Ahmad, Eman, Mohammed” for their encouragement.
- ✓ Team of Al-Quds Open University for their Encouragement.

Acknowledgement

I would like to thank Dr. Fady for his endless support and Kind encouragement throughout the period of his supervision on my thesis.

Appreciation and thanks are also extended to committee members, for their time and effort in reviewing this work.

Special thanks are expressed to my friends for their help and encouragement.

Special and sincere respect, gratitude and appreciation are expressed to my colleagues at work for their support in completing my thesis and making this study possible.

I wish to express my sincere gratitude and warmest love to my family who were extremely supportive and encouraging at times I felt like I will give up.

I am grateful to engineering management staff and to all my master colleagues, who provided all possible support with this thesis.

I am also grateful to all people who in one way or another contributed and assisted in achieving my work successfully.

الإقرار

أنا الموقع أدناه مقدم الرسالة التي تحمل العنوان:

Information Security Management in Palestinian Banking

إدارة أمن المعلومات في البنوك الفلسطينية

أقر بأن ما اشتملت عليه هذه الرسالة إنما هي نتاج جهدي الخاص، باستثناء ما تمت الإشارة إليه
حيثما ورد، وأن هذه الرسالة ككل، أو أي جزء منها لم يقدم من قبل لنيل أية درجة علمية أو
بحث علمي أو بحثي لدى أية 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:

إسم الطالب :

Signature :

التوقيع :

Date:

التاريخ:

Table of Contents

No.	Title	Page
	Dedication	iii
	Acknowledgement	iv
	List of Tables	ix
	List of Figures	xi
	Abbreviations	xii
	Abstract	xiii
1	Introduction	1
1.1	Overview	2
1.2	Background	4
1.3	Problem Statement	5
1.4	Significance of the Research	5
1.5	Research Aims and Objectives	6
1.6	Research Questions	7
1.7	Research Domains and Research Variables	7
1.8	Research Hypotheses	9
1.9	Research Methodology	11
1.10	Research Contributions	12
1.11	Research Limitations and Challenges	13
1.12	Research Organization	14
2	Literature review	16
2.1	Overview	17
2.2	Information Security	18
2.2.1	Information	18
2.2.2	Concepts of Information Security	20
2.2.3	Objective of Information Security	21
2.2.4	Principles of Information Security	22
2.2.5	Importance of Information Security	27
2.3	Corporate Governance	29
2.3.1	Information Security Obedience	30
2.3.2	Information Security Compliance	30
2.3.3	Information Security Governance	33
2.3.4	Information Security Governance Best Practices	34
2.3.5	Challenges Facing Corporate Governance	35
2.4	Information Security Management	36
2.4.1	Information Security Management Components	36
2.4.2	Information Security Program Development and Management	37
2.4.3	Information Security Management Approaches	38

2.4.4	Unrealistic Optimism on Information Security Management	39
2.5	Information Security Management in Banking Sector	40
2.5.1	Related Studies about Information Security in Banking Sector	40
2.5.2	Palestinian Banking Sector	42
2.5.3	Information Risk in Banking Sector	43
2.5.4	Information Security Management in Palestinian Banking Sector	43
2.6	Information Security Standards	44
2.6.1	Global Information Security Standards and Best Practices	44
2.6.2	Importance of Information Security Standards	46
2.6.3	Standards and Best Practices Used In Research	47
2.7	Effective Information Security Management	48
2.7.1	People	48
2.7.2	Process	54
2.7.3	Products/Technology	58
2.7.4	Partners/Suppliers	61
2.7.5	Data	65
2.8	The Economic Approach of Information Security	67
3	Research Methodology	70
3.1	Research Design	71
3.2	Research Data	73
3.3	Data Collection	73
3.4	Research Population	74
3.5	Research Sample	75
3.6	Research Tool	75
3.7	Questionnaire Sections	76
3.8	Pilot Study	77
3.9	Reliability	78
3.10	Validity	80
3.11	Statistical Analysis	82
3.12	Ethics	82
3.13	Research Limitation	83
3.14	Research Procedures	84
4	Data Analysis and Discussion	86
4.1	Data analysis	86
4.2	Statistical Methods	88
4.3	Sample Characteristics	88
4.3.1	Qualifications	88
4.3.2	Specialty	89

4.3.3	Experience	89
4.3.4	Information Security Certifications	90
4.3.5	Work Field	91
4.3.6	Number of the Bank Branches/Offices	91
4.3.7	Information Security Management Standard	92
4.4	Research's Questions and Hypotheses	92
4.4.1	Current State of ISM in Palestinian Banking Sector	93
4.4.2	Influence of Research Domains on the Effectiveness of ISM	100
4.5	Discussion	123
5	Conclusions and Recommendations	131
5.1	Overview	132
5.2	Research Contribution	133
5.3	Recommendations	136
5.4	Future Studies	139
	References	140
	Appendices	163
	Appendix A	163
	Appendix B	165
	Appendix C	172
	Appendix D	173
	المخلص	ب

List of Tables

No.	Title	Page
3-1	Cronbach's Alpha Internal Consistency	79
3-2	Cronbach's Alpha Coefficients of the Questionnaire	79
3-3	Correlation Coefficients for Internal Harmony of the Questionnaire	80
4-1	Likert Scale	87
4-2	Scaling Degrees	87
4-3	Respondents' Qualifications Representation	89
4-4	Respondents' Specialty Representation	89
4-5	Respondents' Experience Representation	90
4-6	Respondents' Carrying Certifications' Related to Information Security Representation	90
4-7	Respondents' Work Field Representation	91
4-8	Respondents' Number of The Bank Branches/Offices Representation	92
4-9	Respondents' Banks Holding International ISM Standard Representation	92
4-10	Application Degree for Section Two Controls	94
4-11	Number of the Bank's Branches/Offices	97
4-12	ANOVA Test for Number of the Bank's Branches/Offices	97
4-13	LSD Post Hoc Tests for Number of Branches/Offices	98
4-14	Banks Holding ISM Standard	99
4-15	People Effectiveness Degree	101
4-16	Process Effectiveness Degree	102
4-17	Product/ Technology Effectiveness Degree	103
4-18	Partners/Suppliers Effectiveness Degree	104
4-19	Data Effectiveness Degree	104
4-20	Section Three Effectiveness Degree	105
4-21	Section Three & Qualification Statistics	107

4-22	ANOVA Test for Qualification	109
4-23	Section Three & Specialty Statistics	110
4-24	ANOVA Test for Specialty	112
4-25	LSD Post Hoc Tests for Specialty	114
4-26	Section Three & Experience Statistics	116
4-27	ANOVA Test for Experience	118
4-28	T- Test for Experience	119
4-29	Section Three & Work Field Statistics	121
4-30	ANOVA Test for Work Field	123
4-31	Research Domains Effectiveness Degree	125

List of Figures

No.	Title	Page
2-1	The CIA Triad	22
2-2	Framework for an Information Security Management System	46
2-3	Achieving Effective ISM Through the Four Ps	48
4-1	Rank of the Five Domains Depending on the Means	126
5-1	Research Domains	136

Abbreviations

Abbreviation	Definition
ANOVA	Analysis of Variance
BCM	Business Continuity Management
BS	British Standard
CIA	Confidentiality Integrity Availability
COBIT	Council for Bibliographic and Information Technologies
DLP	Data-Leak Protection or Prevention
DSS	Data Security Standards
HR	Human Resources
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISF	Information Security Forum
ISM	Information Security Management
ISO	International Organization for Standardization
IT	Information Technology
KGI	Key Goal Indicator
KPI	Key Performance Indicator
KRI	Key Risk Indicator
NDA	Non-Disclosure Agreement
OECD	Organization for Economic Cooperation and Development
PCI	Payment Card Industry
PDA	Personal Digital Assistant
PDCA	Plan-Do-Check-Act
PMA	Palestine Monetary Authority
SPSS	Statistical Package for the Social Sciences

Information Security Management In Palestinian Banking

By

Abdellateef L. Muhsen**Supervisor****Dr. Fady Draid****Abstract**

Recently, organizations' reliance on technology, communications and information has been increased, and this is accompanied with the increase of cyber threats and social engineering. Therefore, information security issues not only occupy high importance in management plans of organizations, but also in the strategic planning of organizations.

Banks are considered as one of the most important sectors that depend on information, and are one of the most significant sectors in Palestine; therefore, information security management in Palestinian banking was selected for this study.

The aim of this study is to examine and review the current state of information security management in Palestinian banks, and measure the application degree of information security management controls in this sector, as well as to highlight issues related to information security management such as governance, compliance and risk. In addition it aims to identify respondents' point of view on the degree of influence of research domains (People, Process, Product/Technology, Partners/Suppliers and data) on the effectiveness of information security management.

The researcher used the descriptive analysis methodology, so he designed a questionnaire distributed to the staff of information technology and internal

audit departments, working in headquarters in Palestinian banks that are licensed to operate from Palestine Monetary Authority (PMA). Therefore, 94 questionnaires were distributed, but only 82 questionnaires were valid for analysis, with response rate 87%.

Research results showed that Palestinian banks are applying information security management controls in a High degree, but the “training and awareness of employees”, and “Data integrity checking” controls were applied in a Moderate degree. In addition, the study indicated that banks that have (10-19) branches are the highest Palestinian banks in applying information security management controls, and the banks that hold international information security management standard apply information security management controls higher than others.

The research also found that People domain (employees) is the most influential domain on the effectiveness of Information Security Management, and relate this result to a "training and awareness to employees" control were applied moderately; this leads to the need of Palestinian banks to further training courses and information security awareness for employees.

Moreover; the study recommended the Palestinian banks to give more importance to “Data integrity checking” control. The study also recommended the Palestinian banks to follow international information security management standards because of their impact on the application of Information Security Management controls.

Chapter One

Introduction

1. Introduction

This chapter aims to introduce an overview of the research title, research approach, and background. Moreover, this chapter clearly shows the problem statement, research aims and objectives, research questions, research hypotheses, research variables and research methodology. In addition; research contribution, research limitation, research challenges and research organization will be explored in this chapter.

1.1. Overview

In the last decade, the Information Security Management (ISM) depended mainly on the technical control measures. However, researchers have shown that the majority of information security failures occur because of violation of controls by trusted personnel. Therefore, Information Security Management can only be adequately assured if the emphasis goes beyond technical controls, and incorporates business process and organizational issues. Many different frameworks, guidelines, and standards were proposed by researchers, practitioners, consultants, and professional organizations to protect their information assets (Choobineh et al., 2007).

Since Palestine in the development stage and has embraced development rapidly, immature implication of those standards in its organizations has been faced. Thus, we need more investigations related to this issue to study, measure and evaluate the current state.

Depending on upcoming results and by surveying the current state of Palestinian organizations, this research is an attempt to study and analyze the situation; in addition, the researcher attempts to identify the most influential issues on Information Security Management in Palestine banking.

Every organization has different assets; one of those main assets is information. Therefore this information should be secured to save the organization, and ensure the success and progress of their business. Moreover, securing information is required to build bridges of trust between the client of the service and the presenter of the service (Rezakhani et al., 2011).

The bank is an establishment that holds the client's bank account in order to enable him to pay and to get paid by third party. Banking business relies increasingly day by day on the information technology. Accordingly, information security has become an essential part for their business success and improvement(2013 مصلح). Therefore, this study focuses on the Information Security Management in the Palestinian banking.

This research aims to form a starting point for conducting more advanced Information Security Management studies and frameworks, which could be applicable and compatible with the Palestinian banking sector as well as other organizations.

1.2. Background

Information Security Management is primarily concerned with strategic, tactical, and operational issues. Those issues are surrounding the planning, analysis, design, implementation, and maintenance of an organization's information security program. Most of salient issues include asset valuation, auditing, business continuity, planning, disaster recovery planning, ethics, organizational communication, policy development, project planning, risk management, security awareness education/training, and various legal issues such as liability and regulatory compliance (Muller et al., 2011).

Information Security Management is a relatively immature discipline. Therefore additional academic study and researches are required. In addition there is a growing need for research to verify/confirm the management challenges, discover current management deficiencies, identify best practices, devise methodologies, and specify requirements for the management of information security (Yeniman Yildirim et al., 2011).

Authors of a case study on banks in Gaza Strip titled "Threats that affect computerized accounting information systems: as A Case study of the banks in Gaza Strip – Palestine. 2008", claim that threats occur but in low frequency. The main reason behind the threat was the lack of expert employees responsible for technology management in the Gaza strip. Therefore they recommended to enhance the employees' ability in IT and

information security in order to control the security tools, and assuring work continuity and information availability (بحيصي & شعبان, 2008).

1.3. Problem Statement

There is almost an absence of relevant Palestinian standards in banks' Information Security Management. Moreover, the importance and sensitivity of information security "especially" in the banking sector and its relation to national security have become very crucial to the development sector worldwide. Therefore, collecting and analyzing the current state of information security management practices can help to identify major gaps in information security the target banks of the study.

The research problem could be summarized as follows: "To what extent is Information Security Management in Palestinian banking effective?" by posing this question, this research aims to identify the problems, implications, benefits, gaps and possible improvements in information security management implementation.

1.4. Significance of the Research

The relevance of this research work is of significant importance to the Palestinian banking sector. It represents the first study about information security management in the banking sector.

The research provides an insightful examination of the current state of Information Security Management application. In addition to highlights

issues and deficiencies and identify the most influential issues on Information Security Management effectiveness. Therefore this research could help to improve Information Security Management in the Palestinian banking sector, and consequently improve its performance and customer satisfaction.

1.5. Research Aims and Objectives

First, the research aims to explore the current state of Information Security Management followed by the Palestinian banking sector, and to highlight the major obstacles and deficiencies in Information Security Management implementation and its effectiveness.

Second, the researcher aims to survey the opinion of information technology specialists in Palestinian banks about the five domains of research, which are (People, Process, Product/Technology, Partner/Supplier, and Data), so as to find the domain that influences Information Security Management effectiveness the most.

Finally, the researcher tries to combine the output of current state of Information Security Management and the output of the most important issues influencing Information Security Management effectiveness in order to make contributions in this field.

1.6. Research Questions

Through this research project, the researcher aims to answer the following research questions which have been designed to achieve the research objectives.

- ✓ To what extent are research controls applied in Palestinian banks to achieve Information Security Management?
- ✓ What are the most influential domains and controls that influence the effectiveness of Information Security Management from respondents' point of view?

1.7. Research Domains and Research Variables

The research is planned to measure the current state application degree of Information Security Management controls in Palestinian banks. In addition, it aims to measure the influence of research domains (People, Process, Product/Technology, Partner/ Supplier, Data) on the effectiveness of Information Security Management.

Here we have a brief definition to research controls and research domains:

- ✓ **Controls:** Group of Information Security Management factors adapted from the Payment Card Industry PCI (2013), and were used in the questionnaire.
- ✓ **People:** Employees who work across organizations in dealing with information.

- ✓ **Process:** Procedures used to implement and achieve Information Security Management.
- ✓ **Product/Technology:** Software or hardware used to gain Information Security Management.
- ✓ **Partner/ Supplier:** Third party that deal with organization and affect its information.
- ✓ **Data:** Information converted into binary digital form.

The researcher also wants to examine the existence of any differences in the application degree of Information Security Management controls among banks that can be attributed to:

- ✓ Number of bank's branches.
- ✓ International Information Security Management standard.

In addition, the researcher wants to examine the existence of any differences in the degree of Information Security Management effectiveness of the research domains as perceived by respondents' attributed to respondents':

- ✓ Qualification.
- ✓ Specialty.
- ✓ Experience years.

- ✓ Information security certifications.
- ✓ Work Field.

1.8. Research Hypotheses

The current state of the Information Security Management in Palestinian banks and the influence of research domains on the effectiveness of Information Security Management will be measured in this study through different analytical and descriptive techniques. However, to further investigate the relationship between the degree of the current state application of Information Security Management in Palestinian banks and the degree of its effectiveness utilizing the different research domains. The following hypothesis will be tested to address the objectives of the study.

H1₀: There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between Palestinian banks in applying the Information Security Management controls attributed to **Number of the bank's Branches/Offices** variable.

H2₀: There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between Palestinian banks in applying the Information Security Management controls attributed to **holding International Information Security Management standard** variable.

H3₀: There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between research's domains that influence the effectiveness of Information

Security Management in Palestinian banks from the point of respondents' view, attributed to respondent's **Qualification** variable.

H4₀: There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between research's domains that influence the effectiveness of Information Security Management in Palestinian banks from the point of respondents' view, attributed to respondent's **Specialty** variable.

H5₀: There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between research's domains that influence the effectiveness of Information Security Management in Palestinian banks from the point of respondents' view, attributed to respondent's **Experience** variable.

H6₀: There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between research's domains that influence the effectiveness of Information Security Management in Palestinian banks from the point of respondents' view, attributed to respondent's **information security certifications** variable.

H7₀: There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between research's domains that influence the Effectiveness of Information Security Management in Palestinian Banks from the point of respondents' view, attributed to respondent's **work field** variable.

1.9. Research Methodology

The researcher has used the descriptive analytical approach, which tries to describe and evaluate the extent to which Palestinian Banks are applying Information Security Management controls. In addition, to measure the dominant factors affecting the effectiveness of Information Security Management. Therefore, this approach satisfies the research goals in order to compare and evaluate the results; raising research hopes to publicize a meaningful content to support the available knowledge of the research theme.

In order to achieve that; the researcher utilized both primary and secondary data sources:

- ✓ **Primary data:** the data collected by hand, for the specific research problem, such as the questionnaire that was distributed to the banks.
- ✓ **Secondary data:** the data collected by other researchers, or for other research purposes, including English and Arabic books and references, journals, articles, reports. In addition to the analysis of Palestine Monetary Authority (PMA) and Palestinian banks websites, and previous research studies that have tackled the subject.

1.10. Research Contributions

The findings of this research project constitute basis for Palestinian banks to perform their Information Security Management, where the whole Information Security Management process and factors influencing the effectiveness of Information Security Management are identified.

Palestinian banks can utilize this study to structure their Information Security Management assessment and identify major gaps in their current performance which can be mitigated.

Moreover, researchers can utilize this research as a starting point for further research projects that approach different aspects of the subject, since the subject was not targeted by other researchers before.

The results of this research are of great importance to researchers, Palestinian banks, and PMA. Therefore, this research is considered to be a significant contribution in Information Security Management.

There is a **high** application degree of Information Security Management controls in Palestinian Banks; that is satisfactory but still needs more attention and improvements.

Respondents claim that “People” are considered the dominant domain that influences the effectiveness of Information Security Management with a **very high** degree (85.8%).

Research results show that there is a moderate application degree in “Training and awareness” and “Data Integrity Checking” controls. Therefore; as “People” considered the dominant domain that influences the effectiveness of Information Security Management, training for employees and improving awareness culture is very important and a sensitive issue for Palestinian banks.

There are differences denoting a statistical significance between Palestinian banks in applying Information Security Management controls due to number of bank’s branches and whether the bank holding international Information Security Management standards.

The researcher supplemented additional domain “Data” to the 4Ps framework that was developed by Information Technology Infrastructure Library (ITIL) (Clinch, 2009), and this could be a starting point for developing new Information Security Management framework in future studies.

1.11. Research Limitations and Challenges

One of the main limitations of this research was the lack of prior research studies on the subject which is considered relatively new to the Information Security Management in Palestine, and to the banking sector in the world. This presents an important opportunity for other researchers interested in the subject to explore Information Security Management from other perspectives.

Since the banking sector is very sensitive, and information security is very confidential, there were very difficulties in acquiring information.

According to PMA (2013), there are seventeen banks working in Palestine, and all IT related issues and specialists are places in the headquarters, so the targeted population was small and limited to headquarters in Ramallah.

Information security policy has become a key instrument for managing security in organizations however its impact on improving security has not been evaluated empirically.

1.12. Research Organization

The rest of this thesis is organized as follows:

Chapter two provides a literature review of the state of art in Information Security Management. First we defined information security, and then we explore corporate governance. After that Information Security Management, Information Security Management in banking sector, information security standards, effective Information Security Management, and the economic approach of information security will be discussed.

Chapter three clarifies the research methodology, research design, research data, data collection, research population and research sample. In addition chapter three discusses research tool, pilot study, reliability and validity.

Farther more, it addresses the ethics, research limitation and research procedure.

Chapter four discusses data analysis, statistical methods, answering research questions and testing research hypotheses. In addition it discusses research findings with previews related research.

Last chapter is about conclusions and recommendations. It explores the research contributions, recommendations and future studies.

Chapter Two

Literature Review

2. Literature review

This chapter consists of nine sections; overview, information security, corporate governance, information security management (ISM), ISM in the banking sector, information security standards, effective ISM, and last section is the economic approach of information security.

2.1. Overview

Information security is not a new field, it has a very long history even before the computer existed, and it has been used since human beings learned how to write.

In a global and competitive business environment as the one existing today, firms depend more and more on their information, because it has been proved that information have huge influence on improving the level of competitiveness between firms(Teece, 2010).

For that reason, firms are aware of the huge importance of having adequate information security programs as well as a correct management of information. In spite of the fact that there are still many firms that continue assuming the risk of lacking adequate protection measures, there are many others that have understood the importance of information security management (Sánchez et al., 2009).

2.2. Information Security

The history of information security reaches back to ancient times and starts with the emergence of bureaucracy in administration and warfare. Some aspects, such as the interception of encrypted messages during World War II, have attracted huge attention, whereas other aspects have remained largely uncovered (de Leeuw & Bergstra, 2007).

In this section; information, concepts of information security, objective of information security, principles of information security and importance of information security will be discussed.

2.2.1. Information

Information is the most valuable asset in the organizations' care and is considered a critical resource, enabling the organization to achieve its goals.

“Information is the oxygen of the modern age” (Ronald Reagan, 40th U.S. President) (Guardian, 1989). It has grown to become the lifeblood of most firms today. Therefore the world has moved into the information economy, an economy based on the exchange of knowledge and services rather than physical goods (Flowerday & von Solms, 2005).

According to Dey (2007) information includes all forms of data, knowledge, messages, recordings, conversations, communications, documents, and images. Therefore, every business depends heavily on

information. In most cases, information has become the vital 'asset' called 'information asset' or 'intellectual asset' for any business.

Information is used to drive most business processes, involving employees from the highest to the lowest levels and not just used as an enabler in modern firms today. Thus, information is indeed a critically important and one of the most fundamental assets for the firms. However, information is an abstract asset; it can exist in many forms, electronic, hard copy, verbal etc. (Ozkan & Karabacak, 2010).

Confidential and critical assets need to be protected satisfactorily. If the information asset is critically important to the future existence of the organization, then the protection of thereof should become a Board of Directors' main issue and the top level management should handle the task of protecting such asset (R. von Solms & von Solms, 2006).

Information can be seen as a basic ware, similar to electricity, without it many businesses simply cannot operate. In addition many organizations will be unable to do business without access to their information resources. That being said, protecting information resources often has no direct return on investment (J. F. Van Niekerk & Von Solms, 2010).

According to Furnell (2008), Information Technology (IT) products or systems ought to perform their functions whilst exercising appropriate control of information. In addition to ensure it is protected against accidental or deliberate dissemination, modification, or loss.

There has been a significant shift in the valuation of firms as the world has advanced into the information economy. One of the driving forces behind this shift in market valuations of firms could be the need for increased investment performance. However, regardless of what the driving forces may be; to ensure that information retains its worth, it needs to be secured and the users need to have confidence when basing their decisions on the information (Davenport, 2013).

The banking sector, which is the focus of this research, can be considered a developed and a vital sector in Palestine. This sector relies on information as its core asset, since information technology is used for transactions and other banking processes. Therefore securing information is extremely important in order to achieve the objectives of the banks and guarantee their survival.

2.2.2. Concepts of Information Security

Information Security is such a broad discipline and therefore it is easy to get lost in a single area and lose perspective and focus. The main concept behind information security is that security is only as strong as the weakest link(Sasse et al., 2001).

Sasse et al. (2001), pointed out that “users are the weakest link”. As such, information security is not only a technical issue, but also a behavioral issue involving users. Therefore an abundance of research has been conducted to understand users’ security-related behaviors, such as

information systems misuse or security-enhancing actions mostly in work environment settings (Bang et al., 2012).

According to Ren and Du (2013), information security consists of many components, the core component depends on human cooperative behavior. Employees whether intentionally or through negligence, often due to a lack of knowledge, are the greatest threat to information security.

Johannes Frederick Van Niekerk (2011) points out that without an adequate level of user cooperation and knowledge, many security techniques are liable to be misused or misinterpreted by users.

2.2.3. Objective of Information Security

The objective of information security is protecting the interests of those depending on information technology and communication systems that deliver the information, from harm resulting from failures of security principles “availability, confidentiality, and integrity” (Abu-Musa, 2010).

According to *COBIT* (2007) information security relates to the protection of valuable assets against loss, misuse, disclosure or damage. In this context, “valuable assets” are the information recorded on, processed by, stored in, shared by, transmitted or retrieved from an electronic medium.

Securing information resources does not as a rule generate income for an organization. Business people are therefore rarely interested in how their information resources are protected. From a business perspective, any

solution would be adequate as long as it is cost-effective and takes into account issues such as productivity and ease of use (J. F. Van Niekerk & Von Solms, 2010).

J. F. Van Niekerk and Von Solms (2010) argued that the goal of securing information is in conflict with the normal business goals of maximizing productivity and minimizing cost. Thus security is often seen as detrimental to business goals because it makes systems less usable, the only absolutely secure system is an unusable one.

2.2.4. Principles of Information Security

Information security can be defined in a variety of ways; however, every definition, even if different, may still be correct. Information security consists of 1) **Confidentiality**, 2) **Integrity**, and 3) **Availability** of information. Also referred to as the C-I-A triad (Stewart et al., 2012).

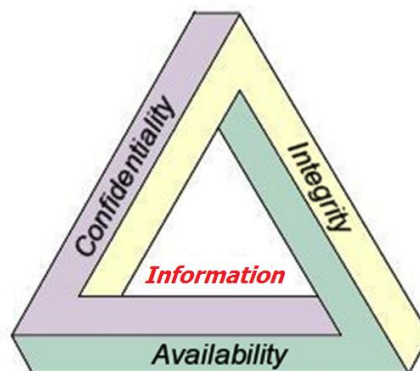


Figure (2-1): Information Security concepts(YOYO, 2010).

The next sections discuss each of the main information security concepts.

Confidentiality

In the context of information security, confidentiality means that information should remain guarded and confidential and only those persons authorized to access it may attain access (Fourie, 2003).

Unauthorized access to confidential information may have devastating consequences, not only to national security applications, but also to commerce and industry in general.

Main mechanisms of protection of confidentiality in information systems are cryptography and access controls. Examples of threats to confidentiality are malware, intruders, social engineering, insecure networks, and poorly administered systems (dos Santos Moreira et al., 2008).

Confidentiality is the privacy of an asset. Specifically, confidentiality can be defined as which people, and under what conditions, are authorized to access an asset. Since the exposure of confidential information could bring about embarrassment to a company or a business and heavy penalties, such information should be assigned a “High” rating, to indicate that the confidentiality of this information is extremely important (Yazdanifard et al., 2011).

Directory information may draw a “Low” confidentiality rating. This information is, for the most part freely available to the public, unless otherwise requested by the user (Shirtz & Elovici, 2011).

Integrity

According to Birgisson et al. (2011), Integrity is concerned with the trustworthiness, origin, completeness, and correctness of information, in addition to the prevention of improper or unauthorized modification of information.

Integrity in the information security context refers not only to integrity of information itself, but also to the origin integrity—that is, integrity of the source of information.

Integrity protection mechanisms may be grouped into two broad types (Stewart et al., 2012):

- ✓ Preventive mechanisms, such as access controls that prevent unauthorized modification of information.
- ✓ Detective mechanisms, which are intended to detect unauthorized modifications when preventive mechanisms have failed.

Fourie (2003) point out that integrity is more difficult to define than confidentiality as there are two primary properties to consider when evaluating it.

- ✓ First, there is the notion that an asset should be trusted; that is, there is an expectation that an asset will only be modified in appropriate ways by appropriate people.

- ✓ The second part of integrity is that in the event that data is damaged, or incorrectly altered by authorized or unauthorized personnel, you must consider how important it is that the data be restored to a trustworthy state with minimum loss.

Information security is liable for the information's integrity. Subsequently, information integrity requires both system integrity and data integrity (Mishra & Dhillon, 2006).

For management to rely on the information within the information systems, assurances need to be provided that the information's integrity has not been compromised, intentionally or unintentionally (Poolsappasit et al., 2012).

Nevertheless, it is not enough to provide assurances months later; it needs to be in real-time. Thus information has its integrity only when the accuracy, completeness, timeliness, validity and processing methods are safeguarded (Fisher et al., 2012).

Stamp (2011) argued that information integrity is dependent on system integrity. In other words, information integrity can be no better than the integrity of the system processing the data or information, although it can be worse.

A system demonstrates processing integrity if “its outputs fully and fairly reflect its inputs, and its processes are complete, timely, authorized and accurate” (Khan, 2012).

To emphasize the two aspects, a system may have integrity but if the data it processes lack integrity at the time the system receives it, then the data will continue to lack integrity when it is transferred to its destination or transformed into information. Thus, to be confident that information, which important business decisions are based on, is trustworthy, both the input data and the processes that are used to produce the information are properly protected (Zissis & Lekkas, 2012).

Protection normally comes in the form of internal controls that result from a thorough risk management process. Risk management therefore plays an important function in ensuring information integrity.

Availability

Availability represents the requirement that an asset be accessible to authorized person, entity, or device. Therefore, despite being mentioned last in the C-I-A triad, availability is just as important and as a necessary component of information security as confidentiality and integrity (Mirkovic et al., 2004).

Natural and manmade disasters obviously may also affect availability as well as confidentiality and integrity of information, though their frequency and severity greatly differ—natural disasters are infrequent but severe, whereas human errors are frequent but usually not as severe as natural disasters. In both cases, business continuity and disaster recovery planning

(which at the very least includes regular and reliable backups) is intended to minimize losses (Stewart et al., 2012).

2.2.5. Importance of Information Security

Computers and networks, particularly the Internet, have become an integral part of everyday life, used for a variety of reasons at home, in the workplace, and at schools. Moreover, most enterprises have become totally reliant on IT; extending outside trusted environments and increasing range of services.

Globalization and technology revolution lead to dependence on computers and networks that are used for communication and for varieties of online interactions and transactions. Therefore information security is required at all levels – the personal level, corporate level, state and country level, it has become the key issue in today's information technology world (Castells, 2011).

New vulnerabilities are found each day, and the evidence of the information threat is growing. Furthermore, those interested in exploiting these vulnerabilities are becoming a well-organized underground (Pfleeger & Pfleeger, 2012).

An increasingly demanding framework of regulation and law, with the increasing concern for safety and integrity of information against attacks, it has become mandatory that organizations follow strict guidelines and

security framework to assure the safety and protection of data and systems (Bruce et al., 2005).

To address these needs, many universities have incorporated information security courses at the undergraduate and graduate levels as part of information systems or computer science majors (Bishop & Taylor, 2009).

Organization's good name is paramount, and the reputation is priceless. Therefore top level management has to protect these from harm. Information security is a board of directors' issue, which is becoming increasingly important as computer networks become more widespread. It encompasses computer- and network related crime, privacy issues, trust and confidence, and dependability of critical infrastructures (Sharma & Sefchek, 2007).

Organizations have a responsibility to protect consumer and organizational proprietary information while ensuring compliance with laws and regulations (IISIT, 2008).

Information security or offering adequate information about security, training and education requires financial resources. Firms do not want to pay for security and they prefer to maintain a physical security they are familiarized with. In fact, recent researches put forward the need to link information security to strategic planning information systems and therefore, to the enterprise objectives (Sánchez et al., 2009).

Information security is an all or nothing issue. For example: are the horses in the field 75% secured if a fence only exists on three of the four sides? Obviously the horses are not secured. In securing information assets and conducting business electronically, it raises information security from a technical issue to a business issue. This highlights the need of embedding risk and control within the culture of the company (Flowerday & von Solms, 2005).

In accordance with the above statement, information security has in fact become a governance challenge and therefore requires all levels within the company to be conscious of the vulnerabilities and risks facing the company (Conner & Coviello, 2004). This has been accentuated by many governments around the world in passing new legislation concerning the safety of information.

2.3. Corporate Governance

Corporate Governance consists of the set of policies and internal controls by which organizations, irrespective of size or form, are directed and managed (R. von Solms & von Solms, 2006).

In this section; Information security obedience, Information security Compliance, Information security governance, Information security governance best practices and challenges facing corporate governance will be discussed.

2.3.1. Information Security Obedience

Information is a fundamental asset within any organization and the protection of this asset, through a process of information security, is of equal importance. Therefore information security obedience explore the relationships between the three fields of corporate governance, corporate culture and information security, and highlight the importance of binding these fields together (Thomson & Von Solms, 2003).

Kotter (2008) defines corporate culture as values that are shared by everyone in an organization, including fundamental beliefs, principles and practices. These fundamental beliefs, principles and practices have a direct influence on the behavior patterns of employees as far as information security is concerned (Kotter, 2008).

Information is an organizational asset, and consequently the information security needs to be integrated into the organization's overall management plan.

2.3.2. Information Security Compliance

Practitioners and academics have started to realize that information security cannot be achieved simply through technological tools. Effective organizational information security depends on all three components, namely: people, processes and technology (Li et al., 2010).

However, with the advances in security technologies, many computing behaviors such as patch management and antivirus updates are now being automated to reduce the task knowledge and time load on end users. However, behaviors such as appropriate use of computer and network resources, appropriate password habits etc., that cannot be addressed by security technologies are often dealt with through organizational computer security policies (Li et al., 2010).

Security breach incidents show that employee negligence and non-compliance often costs organizations millions of dollars in losses. Although, appropriate computer use policies in organizations have been recognized to be important for a long time (Herath & Rao, 2009).

The objective of any organizational policy is to influence and determine employees' course of action. While the defined policies may be crystal clear and detailed, the result may not turn out to be as desired, especially with regard to information security (D'Arcy & Herath, 2011).

The aim of behavioral aspects of security governance is to ensure that employees show conformity with the rules and policies. Since employees rarely comply with information security procedures.

Policies, especially those involving information security, are viewed as mere guidelines or general directions to follow rather than “hard and fast rules” that are specified as standards (Herath & Rao, 2009).

According to Ifinedo (2012) due to the relatively discretionary nature of adherence to policies, organizations find enforcement of security a critical challenge. Thus more recently, research in behavioral information security has started focusing attention to employee intentions to follow security policies.

In organizational information security, responsibility of whether to adhere to organizational security policies or ignore them is delegated to employees. Employees may choose to break security policies for malicious purposes or choose to avoid security policies for mere convenience (Herath et al., 2010).

A study in context of access controls found that employees believe that higher level of information security restricts their ability to follow flexible operation routines, and perceive it as counterproductive. In addition, employee actions related to security policy compliance may also be difficult to monitor (Herath & Raghav Rao, 2010).

Compliances have positioned themselves to be the vital requirements to ensure information security. Thus the rapidly growing use of information technology in various businesses and the transition of sensitive information into digital records have led to the formation of various compliances, guidelines, regulations and regulating bodies (Eastman et al., 2011).

2.3.3. Information Security Governance

Information security governance has become an important business responsibility, and accountability escalated up to the boards of directors' level. Therefore executive management and boards have started realizing that Information Security Governance is becoming their direct responsibility, and that serious personal consequences, specifically legally, could flow from ignoring information security (Spremić, 2009).

According to B. Von Solms & von Solms (2005a) boards of directors will increasingly be expected to make information security an essential part of governance, preferably integrated with the processes they have in place to govern IT, in addition to information security will be properly addressed, greater involvement of boards of directors, executive management and business process owners is required (B. Von Solms & von Solms, 2005).

One of the risks board members are exposed to: 'Failure to understand the impact of security failures on the business, and potential effect on shareholders, share price and competition' (B. von Solms & von Solms, 2005).

Information security governance has become integral to good corporate governance. so company directors should keep in mind that failure and/or refusal to identify and address corporate IT risk may result in personal liability if damages or losses follow (Pfleeger & Pfleeger, 2006).

According to Rastogi and Von Solms (2012) director and even an IT manager may be personally liable for unlimited damages if the failures to identify and manage risks are classified as reckless management of the company by the courts.

2.3.4. Information Security Governance Best Practices

According to Johnston and Hale (2009), it is important to integrate information security governance into corporate governance. Therefore to ensure that organizational goals and objectives are supported by the information security program.

One of the best practices related to information security governance is to establish and maintain an information security strategy. This strategy should be in alignment with organizational goals and objectives to guide the establishment and ongoing management of the information security program. In addition to create an information security governance framework to guide activities that support the information security strategy (Ericsson, 2007).

Developing information security strategy need to identify the internal and external influences to the organization (for example, technology, business environment, risk tolerance, geographic location, legal and regulatory requirements) to ensure that these factors are addressed by the information security strategy (Epstein, 2008).

Finally, defining and communicating the roles and responsibilities of information security throughout the organization to establish clear accountabilities and lines of authority, monitoring, evaluating and reporting metrics (key goal indicators [KGIs], key performance indicators [KPIs], and key risk indicators [KRIs]) to provide management with accurate information regarding the effectiveness of the information security strategy (Parmenter, 2010).

2.3.5. Challenges Facing Corporate Governance

There are many challenges facing the convergence of corporate governance and information security, the most important point is to convince the senior management of an organization that they should be ultimately accountable and responsible for the protection of their organization's information (Thomson & von Solms, 2005).

According to ERIC and Goetz (2007), Board of Directors should be involved in the protection of information, an important organizational asset. The level of information security that the Board of an organization is prepared to propose and put into operation, and the level of information security that is acceptable to the shareholders should be consolidated and result in the corporate information security policy.

The information security policy should be based on the approved corporate security objectives and strategy and is there to provide management direction and support for information security (Radovanovic et al., 2010).

2.4. Information Security Management

Information security management argues that the focus of information security within organizations should be on business and management and not technical issues. Within the technical computer security literature, security policy is used as a synonym for overall security architecture of operating systems; while non-technical security management literature addresses the access control rules for a computer system. Furthermore, Information Security Management should be governed in a comprehensive rather than in project-based manner (Sipior & Ward, 2008).

In this section; Information security management components, Information security program development and management, Information security management processes and Unrealistic optimism on information security management will be discussed.

2.4.1. Information Security Management Components

Information security management can be defined as “a systematic approach that consisting of people, processes, and Information Technology systems, that protects critical systems and information, safeguards them from internal and external threats” (Topi et al., 2010).

Information security management consists of various aspects, such as Information Security Policy, Risk Analysis, Risk Management, Contingency Planning and Disaster Recovery which are all interrelated in some way (Feng et al., 2014).

According to Dey (2007) information security management can no more be done by merely a set of hardware and software. Rather, it requires a complete end-to-end system. In such a way that only authorized and valid users are allowed to access them. Thus strategic approach to Information Security Management will promote a focus on proper management of information as a key resource in global competition (Buchanan & Gibb, 1998).

2.4.2. Information Security Program Development and Management

Developing the world's best information security program is great, but it needs to be effectively managed just like any other operational business unit or department.

Information security objectives are a critical part of business. But unfortunately objectives and intentions are redundant without an action plan. An information security program ties the objectives to specific actions to ensure the required outcomes are reached (Mayer et al., 2007).

Information security programs are logical and well thought out. They provide organizations with a structured way of meeting their information security objectives, such as establishing a 'top down' rather than 'bottom up' approach to information security management (Peltier, 2013). Thus effective information security program must these points in to account:

- ✓ It must be aligned with business needs and protect assets in accordance with business priorities.

- ✓ It must be risk-based and cost-effective.

- ✓ It must be flexible to meet changing business needs and changing threats.

According to Bishop (2012) by utilizing information security programs; firms will be organized by enabling risk based decision making for information security, articulating the links between other functional departments such as HR, IT, etc., and also identification of metrics to measure the effectiveness of information security management.

There are a number of challenges to successfully managing an information security program such as, skill set limitations, limited budget, lack of management support, and general lack of awareness (Randone, 2011).

Formal and professional management of information security program has many benefits, the most important is to ensure there is a strong alignment with the primary objectives of the business, to confirm that the right amount of protection is applied and it is in the right areas (M. E. Whitman & Mattord, 2010).

2.4.3. Information Security Management Approaches

Modern security management approaches can be divided into three groups. The first group includes the approaches that are based on security management standards. The second group is based on best practices and the third is based on more formal approaches (Rezakhani et al., 2011).

A common mentioned problem with most of the above mentioned standards is that they do not provide a process of how to conduct security management but it is merely a checklist. A second problem is the threshold implied by the great amount of pages to read before one can start (Fourie, 2003). Therefore, a more holistic approach is needed.

Research claims and practice have shown that a lot of dimensions have to be considered in security management. To take these dimensions into account a holistic approach that simultaneously considers them is therefore necessary. However, most state-of-the-art security management approaches are not holistic, as most of them only cover parts of the system lifecycle (B. von Solms & von Solms, 2005).

2.4.4. Unrealistic Optimism on Information Security Management

Business environments continue to change with increasing dependence on information technology and widely use of the Internet. This greater connectivity has increased the vulnerability of information systems to various information security threats. In addition, challenges associated with information security are far from resolved, due to lack of managers and user awareness as the major obstacles to achieve a good information security posture (Gupta & Hammond, 2005).

Awareness of information security is the attention 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 (Castells, 2011; Rhee et al., 2012).

according to Rhee et al. (2012), in order for managers to understand the need for information systems safeguards and to exercise necessary security practices, they must perceive their own vulnerability associated with the information system. Therefore the problem is that in many negative situations, people demonstrate a tendency to believe that they are less at risk than others. This underestimation of the likelihood (or probability) of experiencing negative events is called optimistic bias.

Optimistic bias relates to a perception of personal invulnerability. Optimistic bias represents a defensive distortion that could undermine preventive action, interfere with precautionary behavior, and aggravate users' risk-seeking tendency (Rhee et al., 2012).

2.5. Information Security Management in Banking Sector

In this section; related studies about information security in banking sector, Palestinian banking sector, Information risk in banking sector and Information security management in Palestinian banking sector will be discussed.

2.5.1. Related Studies about Information Security in Banking Sector

- ✓ Sinclair et al. (2008), in their field study “**Information Risk in Financial Institutions**”, discussed that “the challenges facing

developers and managers in enabling appropriate information access in these data-driven firms, as they argued that, “The changing organization environment, information accessibility, and regulatory environment all contribute to these challenges”.

- ✓ Bauer (2012), in his paper “A Literature Review on Operational IT Risks and Regulations of Institutions in the Financial Service Sector”, the term “operational risk” is defined as “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk”.
- ✓ (مصالح, 2013) in his field study “**Security of Accounting Data and information and its automated storage Means at Jordan Banks**”, found that, “the compliance rate with hardware and place security of storage means was very high, 94.4%, the compliance rate with individuals security was 95.7%, the compliance rate with system and software and hardware and applications security was 95.1%, the compliance rate with computers and machines and communications was 93.2%, and the compliance rate with intact keeping methods of data in the storage process was 93.8%. The results indicate that the present protection procedures of accounting data and information are adequate and comprehensive”.
- ✓ Roos (2013), in his PhD. Thesis titled “**Governance responses to hacking in the banking sector of South Africa**”, pointed out that

“the board of directors is not fully embracing its IT governance responsibilities and that IT matters are mostly dealt with by risk management committees at board level or IT steering committees at executive management level. The effect of IT risks on business risks such as human resource risk and physical risk is underestimated”.

2.5.2. Palestinian Banking Sector

Banking sector in Palestine is managed by Palestinian Monetary Authority (PMA) which is "The emerging Central Bank of Palestine", due to the special situation of occupied Palestine.

Its main purpose is to ensure the effectiveness of the Palestinian financial system (PMA, 2013), and that via sustaining the economic and financial growth of the Palestinian economy through the following:

- ✓ Effective regulation and transparent supervision of Banks operating in Palestinian territory.
- ✓ Development of Monetary Policies designed to achieve price stability.
- ✓ Focusing on the implementation and operation, into modern and efficient payment systems.

Currently, there are seventeen banks operating in Palestine through a network of more than two hundred branches and representative offices. Appendix A, show all details about Palestinian banks.

The banking sector is important and vital sector in all societies, and it is often a target for theft and fraud, for this, researcher decided to search for this topic of utmost importance.

2.5.3. Information Risk in Banking Sector

Financial institutions in recent years have introduced many new services to make their customers' lives easier. Innovations such making payments online and communicating through mobiles and tablets bring real value to their customers, with great efficiencies and cost savings. On the other hand, those same advances also put institutions at a higher informational risk (Ensor et al., 2012).

According to Bit9 (2014): 47 percent of surveyed organizations know they have suffered a cyber-attack in the past year; 70 percent say they are most vulnerable through their endpoint devices; And yet 52 percent rate at "average-to-non-existent" their ability to detect suspicious activity on these devices.

2.5.4. Information Security Management in Palestinian Banking Sector

There are no previous studies about information security management in Palestinian banking sector, and most of the published studies, have addressed related topics such as e-services or topics related to banking operations.

Thus, this research could be considered the first research in this field to study the status of information security management in Palestinian banks, as well as the factors influencing the effectiveness of information security management process.

2.6. Information Security Standards

Standards often define the characteristics of products and services. They are developed in an open process, reflecting the views of many stakeholders including technical experts, government representatives and consumers. The more active consumers are in developing standards, the more likely it is that products and services meet their need (M. Siponen & Willison, 2009).

In this section; Global information security standards and best practices, Importance of information security standard, and finally standards and best practices used in research will be discussed.

2.6.1. Global Information Security Standards and Best Practices

Information security is a concern for all organizations across the world, necessitating the sharing of global intelligence. A balance between security and privacy, that is acceptable to the majority of the community worldwide, must be found (Sipior & Ward, 2008).

According to Dey (2007), the rapidly growing use of information technology in various businesses and the transition of sensitive information

into digital records have led to the formation of guidelines, standards, and best practices.

The new version International Standards Organization / International Electro-technical Commission (ISO/IEC 27001:2013) specify the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature (ISO®, 2013).

ISO 27001 is not a technical standard but rather a business standard that helps establishing an infrastructure for improving information security continuously in an organization (Ozkan & Karabacak, 2010).

According to Dey (2007), most standards adopts Plan-Do-Check-Act (PDCA) model which is an iterative four-step management method used in business for the control and continuous improvement of processes and products that is reflecting the principles as set out by the Organization for Economic Co-operation and Development (OECD) in 2002.

Information Technology Infrastructure Library (ITIL) describes a cycle as shown in Figure (2-2) with the following steps: Control, Plan, Implement, Evaluate and Maintain.

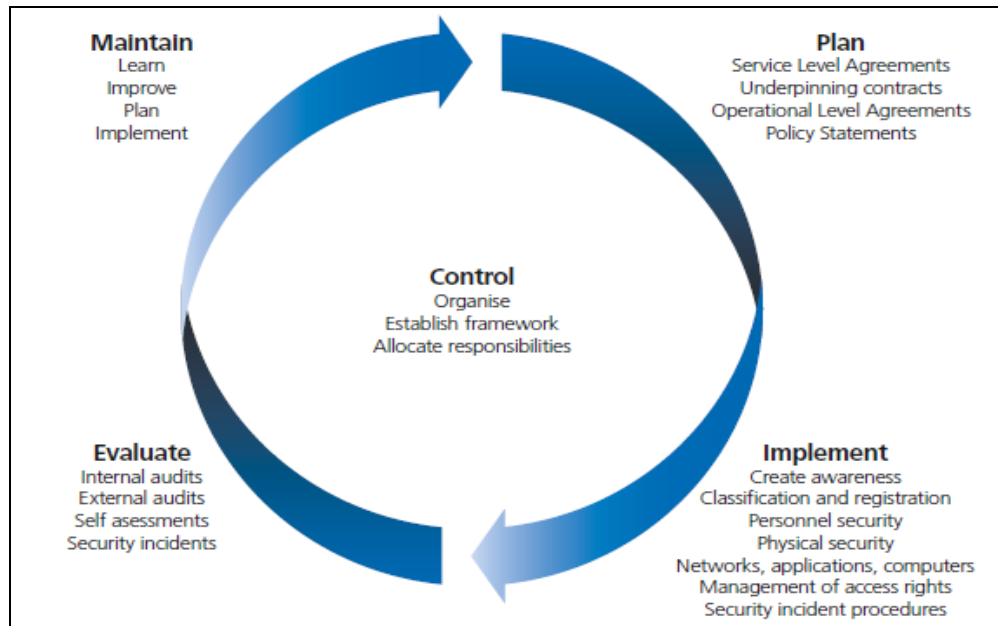


Figure (2-2): Framework for an Information Security Management System, (Clinch, 2009).

Information security standards address people, processes and IT systems to assist in identifying, quantifying and managing threats to information. Appendix (D) contains the main international standards and best practices.

2.6.2. Importance of Information Security Standards

Organizations need to establish the compliances, regulations and audit standards according to their nature of businesses. In addition; to demonstrating alignment with security policies and procedures, Violation of these regulations may be subject to unacceptable audits, penalties, liabilities, punishments to C-Level executives, and even complete closure of business (Dey, 2007).

ISO/IEC 27001 standard provides a robust model for implementing the principles in earlier guidelines. It governs risk assessment, security design, implementation, security management and reassessment (Boehmer, 2008).

Standards provide systematic management approach to adopt the best practice controls, quantify the level of acceptable risk and implement the appropriate measures which protect the confidentiality, integrity and availability (CIA) of information (Jones & Learning, 2011).

2.6.3. Standards and Best Practices Used In Research

There is an ever-growing list of global standards in Information Security Management. Therefore this research, the mainly adopted standards in forming the questionnaire were:

- ✓ ISO/IEC 27002, which is a renumbering of ISO/IEC 17799 that based on BS 7799. ISO / IEC 27002:2005 provide a commonly accepted security architecture framework of guidelines and general principles for developing organizational security standards and effective security management practices (ISO®, 2013b).
- ✓ Information Technology Infrastructure Library (ITIL), which is a framework of best practice guidance in Information Technology Service Management (ITSM). It describes processes, functions and structures that support most areas of IT Service Management, mostly from the viewpoint of the Service Provider.
- ✓ Payment Card Industry (PCI), Data Security Standards (DSS) - govern the security standards for the most payment industries (Visa, MasterCard, etc.)

2.7. Effective Information Security Management

Information security management has been developed to ensure that information is protected at all stages of all business processes. A useful perspective that divides up the scope might be the ITIL ‘Four Ps of Service Design’ shown in Figure (2-3).

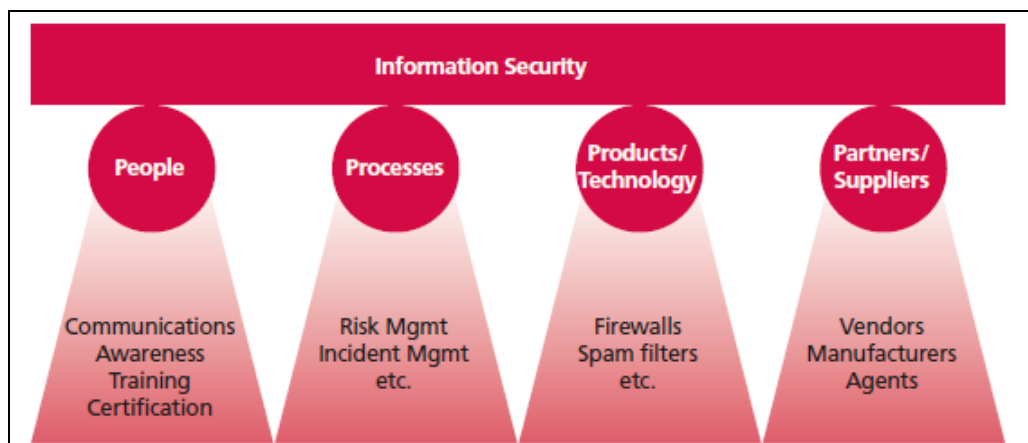


Figure (2-3): Achieving effective ISM through the four Ps, (Clinch, 2009)

Our contribution in this research was the addition of the fifth domain “**Data**”, so the research’s domains will be (People, Process, Product/Technology, Partners/Suppliers and Data), and the researcher aims to study the influence of each domain on the effectiveness of information security management.

2.7.1. People

There are very different ideas and interpretations of the role of the human in security, there are also widely different views of what information needs to be secured and how this could be achieved.

People; the first research domain, and researcher want to find the influence of this domain on the effectiveness of information security management. Thus in this sub section Human element, Role of users in information security, Information security awareness, and security behaviors will be discussed.

Human Factor

Information security basically focuses on protecting resources from external threats and takes insider attacks lightly. However, researches have been shown that a large number of information privacy threats are posed by insiders including organizations themselves (MacKinnon et al., 2013).

Many International researches have shown that technical resolutions are not sufficient to control insider threats. Therefore changing security culture and increasing awareness is very necessary for that (Flynn et al., 2014).

Da Veiga and Eloff (2010) argued that there are a number of papers conclude that insiders -people inside the organization- pose a threat to the protection of information . Therefore organizations need to pay serious attention to reduce the risk that employees pose.

Reliable technical infrastructure, trusted internal processes, good corporate governance and other security measures are among the cornerstone aspects to be considered when aiming to reduce the intentional and unintentional damage caused by employees (McIlwraith, 2006).

Policies and procedures of the Information Security Management are carried out by employees, and that most security failures are related to errors caused by employees (M. Siponen et al., 2014).

According to Corpuz and Barnes (2010) the biggest security threat results from malicious or negligent employees or from faulty controls and oversight. Thus organizations interest to hire employees whose individual actions, concerns, and perceptions are congruent with professional values.

Schumacher et al. (2013) recognizing the consequences of the Information Security Management on employees and the organization is critical. Security practices of employees should be placed within the more holistic security management decision-making context.

Role of Employees in Information Security

A user can be characterized as a person with legitimate access to the organization's information systems. Organizations recognize that their employees and users must protect information, as privacy breaches by employees can be an unwitting avenue to noncompliance (Harkins, 2012).

Information security function of each user is an important part of information security. Users are often the weakest link in the information security chain, as users might be the least reliable barrier to prevent unwanted incidents(Sasse et al., 2001).

Dhillon and Backhouse (2001) have argued that the role, responsibility and integrity of users are important principles of information security management in new forms of organizations.

Users should play an active part in the information security work by preventing unwanted incidents; protecting an organization's material and immaterial assets; and reacting to incidents (Lean-Ping & Chien-Fatt, 2014).

Users can contribute with several security actions in their daily work, e.g. locking the computer when absent from it; password etiquette; cautious use of e-mail and Internet; avoid using unlicensed software; cautious use of organizational assets when working outside the organization; and reporting information security breaches (Line et al., 2011).

The behavior of Loss prevention is created by a combination of several factors: personal characteristics; administrative structures; technological and physical inscriptions; and social norms (Line et al., 2011).

Albrechtsen (2007) argues that possible information security weaknesses related to user behavior should not only be explained by individual failures and violations but rather by mechanisms in the individual's context that generates the behavior.

The field of information security has traditionally mainly been directed towards technological problems and solutions, and has lacked attention to socio-organizational and human aspects (Albrechtsen, 2004).

Consequently, an important part of information security management is to deal with and to understand users' function within their work context Besnard and Arief (2004).

Information Security Awareness

The Information Security Forum (ISF) defines information security awareness as the extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organization, and their individual security responsibilities (A. Jones, 2006).

Security risks that associated with information technology are a topic that has become increasingly of concern. Therefore security-aware culture, referred to as an information security culture, develops as a result of employees' interaction with information security controls such as passwords, access cards or anti-virus software. In addition information security culture can be defined as the way things are done in the organization to protect information assets (Da Veiga & Eloff, 2010).

According to Kruger and Kearney (2006) the goal of a security awareness is to highlight the importance of information systems security and the possible negative effects of a security breach or failure.

The effective management of information security requires a combination of technical and procedural controls to manage information risk. The value

of controls usually depends on the people implementing and using them (Breier & Hudec, 2013).

The implementation of effective security controls is thus dependent upon the creation of a security positive environment, where everyone should be engaged in the behaviors that are expected of them (Al-Awadi, 2009).

M. Whitman and Mattord (2013) classify information security awareness as a dynamic process, and so any awareness program needs to be continually measured and managed to keep abreast of changes in risk profiles.

Security Behaviors

Behavior of employees should be followed, so as to protect information assets it is important to remember that it is necessary to consider a variety of controls and not only technical measures (Risvold, 2010).

One of the security behaviors that we focus on is the creation and use of passwords on an everyday basis, although alternative techniques such as graphical passwords and the use of passphrases potentially offer more secure methods of authentication, passwords are still the most popular measure for protecting information (Sui et al., 2012).

Despite this, many problems with password usage and examples of bad security practice have been observed. Therefore choosing long passwords that are not in the dictionary puts an additional memory load on the user but yields little benefit if accounts are locked out after a fixed number of

failed logins (Duggan et al., 2013). Further, even in instances (e.g. phishing) where the users' bank details could be compromised, the proportion of users actually affected is very small and banks typically reimburse customers who are victims of fraud (Duggan et al., 2012).

Understanding the constraints that users operate under can help explain and/or help reduce the possible explanations for this bad practice. So, for example, limitations in memory capacity can constrain the length and number of passwords that users can remember (Dunphy, 2013).

2.7.2. Process

According to Yeniman Yildirim et al. (2011) security process is the set of rules which help to define acceptable security levels in enterprises or associations.

In this subsection; information security process, information security policy, business continuity management and information risk management will be discussed.

Information Security Process

Information security process is different for every institution. It's usually including general statements of rules and applications regulating the liability of employees, security control tools, aims and goals, and management. (Yeniman Yildirim et al., 2011).

According to (Peltier, 2013) it is essential for an enterprise to define information security requirements, so as to determine appropriate management actions and privileges, and provide guidance for implementing appropriate controls to manage information security risks and provide necessary protection against these risks.

The most important aspect of information security process is its documentation and the establishment of the rules of technology use as well as the codification of the enterprise's information values to all employees from ordinary users to the managers throughout whole enterprise (Commission, 2013).

Information Security Policy

Schumacher et al. (2013) it is better if network security policies can be formed before establishing the process that will be resolve a possible security problem. In addition this is also easier than forming the security policy of an established system.

In order to manage security effectively, both social and technical factors need to be considered concurrently. Security policies integrate these elements into a cohesive plan that organizations use for enforcing security (Goel & Chengalur-Smith, 2010).

Creating a security policy involves gaining an understanding of the organization's mission and assessing its needs for information security for deployment of appropriate security controls (Peltier, 2013).

Ratner et al. (2013) defines security policies as social, political, legal, - economic, and technological stipulations about security enforcement in an organization. Security policy development should be an iterative process where the policy is incrementally refined and its impact on the organization measured.

There are guidelines for the creation of good policies; however, the metrics to characterize or measure the resultant policies are unavailable. It is thus difficult to find out if the policy is effective in managing security or what impact a policy had in improving security (Goel & Chengalur-Smith, 2010).

Business Continuity Management (BCM)

Business continuity management is the identification of potential business risks while trying to avoid, minimize or prepare for these risks, so as to continue business processes and services without interruption. It is a socio-technical approach, in which the emphasis is on preparation for possible continuity problems. Therefore, it has strategic implications for preserving the value of the organization. Service disruptions have been discovered to have significant negative effects on customer loyalty (Sawalha, 2011).

BCM also includes social aspects, not just technical backups, thus, an awareness of the importance of business continuity is essential for ensuring disruption-free operations (Järveläinen, 2013).

Although, BCM literature has focused on the development and planning of business continuity in a single organization, its diffusion and standardization within organizations as well as their internal IT relationships should also be studied, especially within networked corporations.

Information Risk Management

The organization's information risk management approach must be aligned with organizational goals. In addition it must be understood and supported across the senior management of the organization, as regular reporting to management is essential to demonstrate the value provided by effective information risk management practices, and effective information risk management programs contribute directly to successful organizational outcomes and sustainability (Hoo, 2000).

Risk management programs must be provided with sufficient top management support and resources to ensure they are effective to achieve the wanted goals. Therefore information risk management programs are seen by executive and operational management as positive contributors to the success of the organization and not just as another cost of doing business (Peltier, 2013).

It is necessary for management to take decision on applying resources, to manage the company's risk and the auditors should be in agreement.

The risk management process attempts to balance risk against the needs of the company. The goal should be to mitigate the risk to an adequate level as no company can afford the resources to control risk to a zero level (Roos, 2013).

2.7.3. Products/Technology

Computer security is a balance between protecting information and enabling authorized access. Tightening security by making systems more inaccessible can hinder employees and make them less productive. It can also result in lower security as workers struggle to find ways around the security conditions to enable them to do their jobs (Post & Kagan, 2007).

In this subsection some of issues related to technology, such as secure remote management, cloud computing, physical and environmental security management, communication and operation management and access controls management will be discussed.

Secure Remote Management

Analyzing the requirements trends and implementation of information sharing needs has dramatically increased demand for secure remote access to multiple IT operations within the enterprise or large government entities. Additionally, when working with the virtualized services, organizations tend to create a need for more remote infrastructures (Oberheide et al., 2008).

The increasingly mobile work and warfighter force led system administrators to increase the role of remotely managed service as service provider instead of local management of assets. In addition to the increase of configuration Control, consistent patching, and reduced administrative costs comes with a price of perceived lower security because of the increased access to the systems control mechanisms (Farroha & Farroha, 2010).

According to Stouffer et al. (2011) this situation needs to be mitigated by stronger access controls mechanisms, increased monitoring, increased auditing and more passive and positive control over the assets. Many organization and research facilities are developing highly secure remote management methods and products to allow system administrators control over local, virtualized and shared assets in serving the organization's mission.

Cloud Computing

Enterprise strategists have shown strong interest in cloud computing even though initially a lot of confusion about the definition of a cloud. More recently there has been a general agreement that cloud computing represents a shift towards delivering dynamically scalable IT resources as services over the internet (Weinman, 2012).

The main types of architecture are represented by a public and private cloud. Therefore if an enterprise decides to host cloud services in their own

data center, that is considered a private cloud, but if they use cloud services hosted by service providers, it is probably a public cloud (Farroha & Farroha, 2010).

According to Jansen and Grance (2011) security of cloud computing is the biggest concern Enterprise. Thus information Security, isolation, and multi-tenancy are key requirements of any cloud. Therefore applications and users are more comfortable using private cloud especially when dealing with secret or sensitive data, or data that is protected by privacy laws like healthcare and financial data.

The Enterprise can include private, public and hybrid cloud structure to process and store varying levels of sensitive information. Thus since private clouds are placed behind the company firewall, the risk here is more internal within the company (Mather et al., 2009).

Physical and Environmental Security Management

Physical security concerns with hardware. Whereas environmental security interests in computer center, delivery area, collection area, disposal/removal points, fire protection, air conditioning, cables, power supply, locks and alarms. In addition to establish log registry system for users, visitors and equipment coming in or going out of information facility areas (Dey, 2007).

Communication and Operation Management

In order to ensure security and correctness of information processing, write down procedures and responsibilities for all related operations including housekeeping, change/update management, segregation of duties, software or service acceptance and deployment criteria (in-house, outsourced), network protection (wired, wireless, mobile). In addition to e-commerce , clock synchronization, backup, recovery, exchange or transfer of data media, exchange of communication, use of e-mail, fax and handling of public information. State monitoring mechanisms including maintenance of audits and logs (Al-Mayahi & Sa'ad, 2014).

Access Controls Management

Define procedures and responsibilities for all access related tasks. This will include user creation/registration for network (wired, wireless, mobile, and dialup), operating system, application and databases, allocation of rights and privileges. In addition to use of system utilities, port open/close criteria, monitoring of password, and access to critical systems, etc. Monitor access to information by maintaining audits and logs (Singh, 2012).

2.7.4. Partners/Suppliers

Organizations can outsource their IT infrastructure and have interorganizational information systems, but they cannot ignore the

possible risk to their reputation if their external partners fail to provide the service required of them (Järveläinen, 2013).

In this sub section; issues related to third parties like partners and suppliers such as contracts, audits, technical methods, training and new technology adoption will be discussed.

Contracts

Business dictionary defines contracts as: A voluntary, deliberate, and legally binding agreement between two or more competent parties. Contracts are usually written but may be spoken or implied, and generally have to do with employment, sale or lease, or tenancy (Järveläinen, 2013).

In the contracts, clients require disaster recovery plans from the vendor, which are tested regularly and audited by the client or a third party. The managers understood that Information Security Management can preserve the value of the company, and reliable service increases the trust of customers (Kiefer, 2004).

Audits

Audits are used inside organizations to get feedback and update Information security measures. Whereas external audits are used to control vendors and increase the power of the client (Senft & Gallegos, 2010).

According to Järveläinen (2012) auditing was used frequently when selecting a vendor, contract phase or before new system adoption. Some

companies were audited dozens of times a year, although Information security was not always part of the audit. Thus audits used as control mechanisms, to ensure that the vendor was actually trustworthy.

Technical Methods

Technical methods were also used to enhance Information Security in organizations, on both the system and individual level. Therefore the purpose of technical methods is mainly to control and limit damage, but also to transfer responsibility (M. T. Siponen, 2005).

According to Järveläinen (2012) employees of the supplier have to sign a non-disclosure agreement (NDA) and information security policy. Thus, if they access a company's network, a virtual private network and an individual account – restricted to a certain system – is used.

In heavily regulated sectors, a security clearance was made for all employees, including the suppliers' employees accessing the firm's network. Therefore the technical methods were thus used for controlling the users and limiting possible damage.

Training

On the individual level, training was used for improving Information Security Management in inter organizational IT relationships. In addition, training created awareness of and embedded practices for external users working for outsourcing vendors (Leimeister, 2010).

According to (Fenton & Wolfe, 2007) in some cases, when the help desk was outsourced, help desk employees were treated in the same manner as the client's own employees; they went to the same IT training and signed Information policies and NDAs.

New Technology Adoption

For today's organizations, connecting to a complex environment is not a choice, but a necessity in order to survive and thrive. Intense competition requires organizations to be more effective, often by adopting new or advanced information and communication technologies (ICTs) (Baker & Wallace, 2007).

The cost to organizations is that more complex technology requires specialized support and resources, and creates a rich environment for breeding vulnerabilities and risks. Therefore contribution of advanced ICTs is often compromised, because of the unacceptably high levels of security breaches experienced (Qian et al., 2012).

However, most organizations view information security control as an overhead and adopt a reactive management approach. Indeed, "actions taken to secure an organization's assets and processes are typically viewed as disaster preventing rather than payoff-producing" (Brown, 2011).

Caralli et al. (2004) pointed out that "organizations do not routinely require return on investment calculations on information security investments, nor

do they attempt to measure or gather metrics on the performance of such investments.”

2.7.5. Data

Protecting information could have profound business and legal implications. Basically, data became ‘life blood’ on business, and compromising this life blood, could kill the business (Gillies, 2011).

In this sub section; data usage, asset management and data leakage will be discussed.

Data Usage

Information security focuses on providing confidentiality, availability, and integrity to informational assets of organizations. In contrast, the principle of security safeguards in information privacy focuses on achieving a “reasonable” or an “adequate” level of protection of information (Dayarathna, 2009).

Clear understanding of the required level of protection is necessary for choosing appropriate organizational and technological measures for protecting information (Breier & Hudec, 2013).

Asset Management

Asset management interested in identifies information assets with responsible owners and defines rules for the acceptable use of these assets from security point of view. In addition to classify assets using any

standard classification mechanism such as ‘Sensitive’, ‘Confidential’, ‘Private’, and ‘Public’ along with handling, labeling and disposing procedures (Schumacher et al., 2013).

K.-c. Chang and Wang (2011) argued management as part of organizations risk assessment process, is required to consider the risks to the company’s information assets. Once the threats have been identified, risk mitigation needs to take place so that the risks are contained and are at an appropriate level.

Data Leakage

For years, the security industry has focused on outside threats and thus has released products like those for intrusion prevention and malware scanning, focusing on keeping attackers from breaking into government or corporate networks and systems and stealing information, planting malware, or creating back doors for future access (Rodriguez & Martinez, 2013).

According to Lawton (2008) while outside side threats remains a concern, a more recent trend is working on threats emanating from the inside, looking at threats from information leaving an organization without authorization.

Data leakage prevention aims to keep employees and others with access to a system from intentionally or unintentionally sending out sensitive material, such as government or business secrets; intellectual property; research results; confidential e-mails; financial data; and Social Security,

credit-card, and bank-account numbers, from desktop or mobile systems without authorization (Greitzer & Hohimer, 2011).

The approach that vendors have developed to address these problems is known by many names, including data-leak protection or prevention (DLP), extrusion prevention, anti-data leakage, insider-threat protection, and outbound-content management (Shabtai et al., 2012).

In addition; to helping stop data leakage, DLP's content monitoring gives organizations a good look at their daily business communications. This helps them identify patterns and improve their communications processes (Blasco et al., 2012).

Moreover, DLP helps organizations comply with government regulations regarding privacy, the protection of sensitive data, and the maintenance of records. Therefore if a data leak receives a lot of public attention, it could damage an organization's reputation, causing current and potential customers to lose trust (Tipwong, 2011).

2.8. The Economic Approach of Information Security

Business has become increasingly dependent on information and its underlying communication technologies. While several efforts have been undertaken to set up concepts to secure the information infrastructure, security economic plan still lack metrics for decision support (Castells, 2011).

According to Maizlish and Handler (2010), evaluating IT investments should consist of accessible data, reliable information, accurate content, flexibility of the system usage, scalability of the system in adjusting and following business needs, and finally the cooperation of the team and managers in doing their job well.

A key factor in getting value from security is to insure that, the financial returns from a successful implementation of a security-enabled business process should justify the cost of security in terms of enabling business. Therefore generally it is impractical or difficult to dissociate the returns from the business processes (Kleidermacher & Kleidermacher, 2012).

Seker (2012) states that “the costs of implementing security measures must be weighed against the value of information being protected and the price of having a security incident caused by non-implementation of security measures”.

Information security infrastructure is the foundation of a secure environment. In addition it provides a comprehensive plan that protects the confidentiality, integrity, and availability of information resources. Therefore information security plan is composed of risk assessment, technology architecture, policies and procedures (M. Whitman & Mattord, 2013).

Enterprises around the globe are increasingly concerned about the risk in cyber threats and the rising number of incidents shared publicly justifies

their worries. Therefore budgets are being reduced and technology departments are being asked to cut resources. Thus risk up, budgets down. In addition the risk realities are exploited by anyone who uses the downturn in security enforcement to step up the pace of exploitation (Bacik, 2011).

Conclusion

Information security management is not temporary issue or project based, but essential issue and part of strategic planning. Therefore to get effective information security management social side and corporate culture consider as important as technical issues or more.

International standards and best practices formulated in order to govern information security management. Therefore, in this research combination of three standards and best practices made in order to study the influence of research domains (People, Process, Product/Technology, Partners/suppliers and data) on information security management.

Chapter Three

Research Methodology

3. Research Methodology

The aim of this chapter is to describe the methodologies which the researcher follow in order to achieve the research goals. Therefore; research design, research data, data collection, research population and research sample will be discussed. In addition this chapter discussed research tool, pilot study, reliability and validity. Farther more; ethics, research limitation and research procedures also addressed.

3.1. Research Design

A research design is the framework or plan for a study used as a guide in collecting and analyzing data. There are three basic types of research design:

- ✓ Exploratory: used to discover ideas and insights.
- ✓ Descriptive: usually concerned with describing a population with respect to important variables.
- ✓ Causal: is used to establish cause-and-effect relationships between variables

In this research both exploratory and descriptive analytical were used. Therefore; exploratory research used though:

- ✓ Literature review: review of previous studies, article, journal papers, books conferences and internet.

- ✓ Interviews: Interviews with people knowledgeable about the general subject being investigated.

Interviews used in multiple stages:

First stage: interviews used to understand the problem deeply, and to take an idea about the circumstances surround the information security management.

Second stage: after questionnaire was designed, the interviews were made in order to discuss the questionnaire and to rebuild it in the way that could be answered from the banks' employees clearly, in addition to ensuring bank privacy.

Third stage: during the distribution of the questionnaire in order to get the information and the feedback needed to help in analyzing the results of the questionnaire.

Last stage: after collecting the questionnaire, and after analyzing results, in order to help in discusses the result in the right way.

In Addition; this researcher has used the descriptive analytical approach, which tries to describe and evaluate to what extent Palestinian Banks are applying Information Security Management. In addition to what are the dominant factors affecting Information Security Management effectiveness. Therefore 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.

In order to achieve that questionnaire was developed and distributed by hand, after that questionnaire was collected and analyzed.

3.2. Research Data

In this research, the researcher utilized both primary and secondary data sources.

- ✓ Primary data: which is the data collected by hand, for the specific research problem, such as questionnaire that was distributed to the banks.
- ✓ Secondary data: which is the data collected by other researchers, or for other research purposes, including English and Arabic books and references, journals, articles, reports. In addition to analysis of PMA and banks websites, and previous research studies that have tackled the subject.

3.3. Data Collection

The researcher distributed the questionnaire by hand, and then data from the questionnaire was received, after contacting the banks and assuring their willingness to fill in the questionnaires.

170 questionnaires were printed to be distributed to the sample that consists of 17 banks; one bank refused receiving questionnaires, due to the Bank's

policy that prevent filling any questionnaire. Another Bank received the questionnaires and promised to fill but unfortunately they apologized later.

The researcher distributed 94 questionnaires by hand to 16 Banks, but only 82 valid questionnaires were returned from 15 Banks. Hence, the total response rate for this questionnaire was 87% which is an acceptable response rate.

3.4. Research Population

The nature of the Palestinian banks hierarchy is centralized, and all Information Technology (IT) staff exists in the Head Quarters, so the targeted population is only exists in the Head Quarters in Ramallah.

According to Palestine Monetary Authority PMA (2013) banks that are currently recognized to operate in Palestine are (17) Banks (appendix A), these banks classified by PMA to three categories, 1) Local Commercial Banks, 2) Local Islamic Banks, 3) Foreign Commercial Banks(PMA, 2013).

The population of this study is the Head Quarters of the Banks in Palestine that are recognized by Palestine Monetary Authority (PMA), because the targeted population is only exist in the Head Quarters. The research focused on IT and IT auditor staff in those Banks because it discussed the Information Security from the management side (PMA, 2013).

3.5. Research Sample

According to PMA (2013), number of banks recognized to operate in Palestine is (17) Banks when the sample chosen. Therefore the research included all population in collecting the needed data based on internet web sample size calculator (Systems, 1982), list of Palestinian banks on (appendix A).

3.6. Research Tool

As highlighted earlier in literature review, the questionnaire (Appendix B) was build depending on international standards and best practices of information security. In addition; multi stages of adjustments and refinement were made.

Specialists (Appendix C) in several related fields such as IT, Measurement and Evaluation, Information Security, and Management were involved in designing and refining the questionnaire. In addition, applying several stages were conducted before the final edition of the questionnaire was developed, and every change was made after the supervisor approval.

The listed banks in the sample were contacted, and given information about the objective of the research, and they were promised for confidentiality of information. In addition; recommendation paper which has been taken from the faculty of the higher education – An Najah National University proposed to human resources department, which is the official side to receive questionnaires.

Then banks were asked if they are willing to fill in the questionnaire, a period of two months was the process taken to the participating banks to fill in the questionnaire, and some banks were contacted several times during this period to fill in the questionnaire, at the end; two banks out of the seventeen refused to fill in the questionnaire.

3.7. Questionnaire Sections

The researcher used questionnaire because it's the best way to gather numerical data, which could be used to confirm hypotheses. In addition; questionnaire is a simple and rapid tool for collecting data in a reasonable time with a reasonable effort.

Research's Questionnaire was divided into three sections:

First Section:

- ✓ Questionnaire cover, which is divided to two parts: purpose of the questionnaire and letter of gratitude to participants with promises use the information just in the research for study purposes.
- ✓ General Information, which consists of two parts: personal information related to the respondent person and organizational information related to the respondent bank.

Second Section: Status of information security management in Palestinian banks.

The factors (controls) addressed in this section were adapted from “Payment Card Industry (PCI), Data Security Standards (DSS) - govern the security standards for the most payment industries (Visa, MasterCard, etc.)” (PCI, 2013).

This section consists of 25 control statements, so as to measure the application degree of them using five point Likert scales. "1" Very low, "2" Low, "3" Moderate, "4" High, "5" Very high (Jamieson, 2004).

Third Section: Effectiveness of information security management

This section consists of five domains; each domain consists of five controls, to evaluate them using five point Likert scales. "1" Very low, "2" Low, "3" Moderate, "4" High, "5" Very high.

Four of the five domains (People, Process, Product/Technology, Partners/Suppliers) were developed according to Information Technology Infrastructure Library (ITIL) (Adams, 2009). In addition to fifth domain (Data) which was researcher contribution.

The factors (controls) of each domain were adapted from “ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls” (ISO®, 2013; PCI, 2013).

3.8. Pilot Study

Banks have strict policy in dealing with received questionnaire, and varied difficulties in order to get approval to distribute the questionnaire. In

addition; it's almost impossible to get responses from different respondents in the same bank twice; one for pilot study and another for the research.

As mentioned earlier all Palestinian banks are only 17 banks, which represent the whole research population, and the lack of response of any of the banks could adversely relate to the research results.

In addition; it is difficult to exclude responses from one or two banks to use them in a pilot study, as this could make bias in the research results, because of the limited research population.

According to previous justifications, pilot study wasn't done as its traditional form; but instead electronic questionnaires were distributed using Google Docs to respondents working in similar positions, in order to get feedback and insure that questionnaire is clear and understood.

3.9. Reliability

The term "Reliability" is a concept used for testing or evaluating research tool, the idea is most often used in all kinds of research. Therefore; Cronbach's alpha generally used to measure reliability(Golafshani, 2003).

As Cronbach's alpha increased as the intercorrelations among test items increased, and is thus known as an internal consistency estimate of reliability of test scores (Gliem & Gliem, 2003).In this research, the researcher checked reliability of the questionnaire by checking consistency through Cronbach's Alpha test as shown in table (3-1).

Table (3-1): Cronbach's Alpha internal consistency, Cortina (1993)

Cronbach's alpha	Internal consistency
$\alpha \geq 0.9$	Excellent
$0.7 \leq \alpha < 0.9$	Good
$0.6 \leq \alpha < 0.7$	Acceptable
$0.5 \leq \alpha < 0.6$	Poor
$\alpha < 0.5$	Unacceptable

To measure questionnaire reliability the Cronbach's alpha was calculated for all statements in the questionnaire as shown following in table (3-2):

Table (3-2): Cronbach's Alpha coefficients of the questionnaire

Section / Domain	Number Of Factors	Cronbach's Alpha Coefficients (α)	Internal consistency
Section Two	25	93.69%	Excellent
Section Three: Domain One	5	80.85%	Good
Section Three: Domain Two	5	72.16%	Good
Section Three: Domain Three	5	89.22%	Good
Section Three: Domain Four	5	81.27%	Good
Section Three: Domain Five	5	85.21%	Good
Section Three	25	92.49%	Excellent

From the last table (3-2) it's clear that all the questionnaire variables are above 70%, as well as the total reliability of the questionnaire is (95%). Therefore, the research tool is reliable.

Internal Harmony Testing

The researcher has tested the internal harmony of the questionnaire by calculating the correlation coefficients of each question and the total number of the questions for each domain.

The researcher also calculated the correlation coefficients of each domain, in addition to the total number of the domains. Therefore the correlation coefficients denoted significance at (0.01) levels which means a content reliability for what is being measured as shown in table (3-3).

Table (3-3): Correlation coefficients for internal harmony of the questionnaire

Domain	Correlation coefficient	Significance level
Domain One: People	0.662	0.000**
Domain Two: Processes	0.825	0.000**
Domain Three: Products/Technology	0.795	0.000**
Domain Four: Partners/Suppliers	0.811	0.000**
Domain Five: Data	0.826	0.000**

** .Correlation is significant at the 0.01 level (2-tailed).

3.10. Validity

The validity of a research can be examined by assuring that the research has measured what it was supposed to measure, validity of this research was assured through the following means:

- ✓ The researcher involved arbitrators and experts (listed in appendix C), in Information Security and Information Technology as well as a statistician to refine the research tools.
- ✓ Research tool were derived from international information security management standards and best practices.
- ✓ Modifications and adjustments on the research tool were made and discussed deeply with the supervisor. In addition; questionnaire was refined and all comments and advices were taken in consideration in order to assure the efficacy of research tool in achieving the research objectives.
- ✓ The edited version resent to experts and specialists from three banks and one from PMA, in order to review the questionnaire, to make sure that the statements are clear and meaningful. In addition to ensure that questionnaire meets banks privacy and confidentiality.
- ✓ Some modification were added to the questionnaire before achieving the final version, then my supervisor send the questionnaire to attributer from Information Technology college at An-Najah National University, then the questionnaire was ready for distribution.

3.11. Statistical Analysis

Statistical Package for the Social Sciences (SPSS), which is a computer program were used for statistical analysis.

The following statistical descriptive and tests were used to analyze the data, answer the questions, and to test the hypotheses:

- ✓ Frequencies, Descriptive, Means, Standard deviations and percentages to represent the collected data in a meaningful numbers.
- ✓ Independent-Sample T-Test to indicate the significance difference between two level independent variables and to test the hypotheses.
- ✓ One-Way ANOVA to indicate the significance difference between more than two level independent variables and to test the hypotheses.
- ✓ Post-hoc test (LSD) to understand the differences between the surveyed banks due to the specific independent variable.

3.12. Ethics

The researcher followed ethical standards in all research stages:

- ✓ Recommendation paper to every bank which has taken from the faculty of the higher education – An Najah National University.
- ✓ Ensure that the questionnaire is acceptable and recommended from PMA.

- ✓ The interviews were confidential and generalized, without any indication to the interviewee or place of work.
- ✓ The questionnaire did not have any indication to person how filling of name of the bank.
- ✓ Process of distributing the questionnaire was according to banks policy. Therefore the questionnaire applied to human resources department, and then they deliver the questionnaire to specialized departments in order to ensure it's free from any confidential information.
- ✓ Confidentiality was maintained in all process and procedures.

3.13. Research Limitation

- ✓ Lack of prior research studies on the subject, which is considered relatively new to the information security management in Palestine, and on banking sector in the world.
- ✓ Since the banking sector is very sensitive, therefore dealing with information security is very confidential, and need hard effort and communication skills to get information.
- ✓ Dealing with financial institution is very rigid and sensitive, because their work time is limited, and time equal money.

- ✓ There is no previous questionnaire meet the research objectives, so the researcher builds the questionnaire and it take long time and efforts.
- ✓ According to PMA (2013), there is seventeen banks working in Palestine, and all IT related issues and specialists are in headquarters, so the targeted population was small and limited in headquarters in Ramallah.

3.14. Research Procedures

Period of the Study

The study was conducted from Dec 2012 to Apr 2014, but the questionnaire distribution period was from Oct 2013 to Dec 2013.

Place of the Study

The study was applied on the banks that are recognized to operate by PMA.

Conclusion

This chapter has given an overview on the research methodology, population, and sample. In addition it's highlights the importance of research tool. Moreover, it discussed the quality standards for research tool and the procedures of the data gathering.

Chapter Four

Data Analysis and Discussion

4. Data Analysis and Discussion

Questionnaires distribution process has been finished, and the data have been collected and verified in order to identify incomplete and inconsistent responses. So, the next steps are analyzing collected data, and explore the results in addition to discussion.

In this chapter; data analysis, statistical methods, answering research questions and testing research hypotheses will be discussed. In addition to discuss research findings with previews related research.

4.1 Data analysis

Statistical Package for the Social Sciences (SPSS) software was used to analyze data acquired from questionnaire. SPSS is a computer program used for statistical analysis, and has many features and properties which can provide appropriate results; these results lead to achieve research purpose. In addition; SPSS can provide several statistics for each element in the research questionnaire. As well as, SPSS is useful to get the causal relationships between questionnaire elements (DeCoster & Claypool, 2004).

The Likert (1974) five level scale was used in encoding questionnaire, the following table (4-1) clarifies 1-5 Likert scale:

Table (4-1): Likert scale

Scale	Very high	High	Moderate	Low	Very low
Degree	5	4	3	2	1

Responses' average (Mean) for each control, domain or ever section was calculated by SPSS.

The application degree and the effectiveness degree of each control, domain or section were identified by classifying the response averages into five degrees based on what was agreed with the arbitrators, ranging from very low to very high.

These degrees which are based on five intervals were calculated as follows:

The interval length was calculated by dividing the response range (5 which corresponds to very high minus 1 which corresponds to very low) by the number of intervals which is 5, as following: $(5-1)/5 = 0.8$, table (4-2) shows the intervals and there represented scaling degrees used in the research.

Table (4-2): Scaling degrees

Interval	Degree
1.00-1.80	Very low
>1.80 – 2.60	Low
>2.60 – 3.40	Moderate
>3.40 – 4.20	High
>4.20 – 5.00	Very high

4.2. Statistical Methods

The following statistical descriptive and tests were used to analyze the data, answer the questions, and to test the hypotheses:

- ✓ Frequencies, Descriptive, Means, Standard deviations and percentages to represent the collected data in a meaningful numbers.
- ✓ Independent-Sample T-Test to indicate the significance difference between two level independent variables and to test the hypotheses.
- ✓ One-Way ANOVA to indicate the significance difference between more than two level independent variables and to test the hypotheses.
- ✓ Post-hoc test (LSD) to understand the differences between the surveyed banks due to the specific independent variable.

4.3. Sample Characteristics

4.3.1 Qualifications

Table (4-3) shows that most of the respondents have a bachelor degree (74%), and (22%) have a higher educational degree, while (4%) have diploma or less, which means that all respondents are educated and the majority of them have at least bachelor degree.

Table (4-3): Respondents' Qualifications representation

Qualification Degree	Frequency	Percent
Diploma or less	3	4%
Bachelor	61	74%
High Education	18	22%
Total	82	100%

4.3.2. Specialty

Table (4-4) explores that more than half of the respondents have a specialty in Information Technology (IT) (56%), and about fourth of them are engineers (23%), while the last fourth respondents have administration specialties (20%), this indicates that the sample covers the targeted population of the study.

Table (4-4): Respondents' Specialty representation

Specialty	Frequency	Percent
Administration	16	20%
Engineering	19	23%
IT	46	56%
Other	1	1%
Total	82	100%

4.3.3. Experience

It is clear from Table (4-5) that most of the respondents (82%) have at least six years of experience, while the others (18%) have less than six years of

experience, this means that the respondents have a good experience in their working field.

Table (4-5): Respondents' Experience representation

Experience	Frequency	Percent
5 years or less	15	18%
6 - 10 years	22	27%
11 - 15 years	25	31%
More than 15 years	20	24%
Total	82	100%

4.3.4. Information Security Certifications

Table (4-6) shows that most of the respondents (68%) are not carrying certifications related to Information Security; while (32%) of respondents are carrying certifications related to Information Security. Which could be justified by that: not all the respondents are information security specialists. In addition (20%) of respondents have administration specialty.

Table (4-6): Respondents' carrying certifications' related to information security representation.

Certifications	Frequency	Percent
Yes	26	32%
No	56	68%
Total	82	100%

4.3.5. Work Field

From Table (4-7); we can notice that the majority of respondents (52%) are working in the Technical field, and (40%) of them are working in the Administrative field, while the remaining (7%) are working in Both Technical and Administrative Field Simultaneously.

This indicates that information was collected from both administrative and technical perspectives, which is very important for this research because its study the information security from managerial side.

Table (4-7): Respondents' Work Field representation

Work Field	Frequency	Percent
Administrative	33	40%
Technical	43	52%
Both	6	7%
Total	82	100%

4.3.6. Number of the Bank Branches/Offices

Table (4-8) describe the number of the respondent Banks' branches in Palestine, (23%) of respondents are working in banks have 5 branches or less, (21%) of them are working in banks have from 6 to 10 branches, and (29%) of them are working in banks have from 10 to 19 branches, while the other respondents (27%) are working in banks have 20 or more branches. This information indicates that the respondents cover all Palestinian banks.

Table (4-8): Respondents' Number of the bank Branches/Offices representation.

Number of the bank Branches/Offices	Frequency	Percent
5 branches or less	19	23%
6 to10 branches	17	21%
10 to 19 branches	24	29%
20 or more branches	22	27%
Total	82	100%

4.3.7. Information Security Management Standard

Table (4-9) shows that more than half of the respondents' Banks hold International Information Security Management standard (58%), while the other banks (42%) are not, this indicates that most of the Palestinian banks are following international Information Security Management standards.

Table (4-9): Respondents' banks holding International ISM standard representation

certifications	Frequency	Percent
Yes	47	58%
No	34	42%
Total	81	100%

4.4. Research's Questions and Hypotheses

The researcher examined the existence of statistically significant differences between banks in relation to their branches number, or whether they hold an international standard or not. In addition, the researcher examined the existence of statistically significant differences between the Respondents' evaluation to the domains influencing the effectiveness of

information security management, in relation to their Qualification, Specialty, Experience years, Carrying certifications related to information security, and their Work Field.

4.4.1. Current State of ISM in Palestinian Banking Sector

This is the second section of the questionnaire; the output of analyzing this section should answer the research first question, in addition to test research hypotheses that are relevant to the respondent's banks.

Research's first question:

To what extent do research controls applied in Palestinian banks to achieve Information Security Management?

To answer this question, descriptive statistics as shown in table (4-10), used in order to get Means, Standard deviation (S.D.), and application degree for each control and for all controls.

Table (4-10): Application Degree for Section Two Controls

No	Control	N	Mean	S.D.	Application Degree
1.	Definition of information security roles & responsibilities.	82	4.17	0.584	High
2.	The development of information security policies and procedures within the organization.	82	4.21	0.766	Very High
3.	An information and Asset Classification schema such as (Confidential, Private, Personal Public).	82	4.01	0.745	High
4.	Users training & awareness e.g. Internet threats, spear phishing socially engineered email	82	3.37	0.988	Moderate
5.	Management and inventory of authorized and unauthorized devices, systems, software, etc.	82	4.05	0.845	High
6.	Patching, updating and upgrading of applications, device OSs, and operating systems.	82	4.12	0.727	High
7.	Secure configurations on computers. Such as antivirus, encryptions, firewalls.	82	4.66	0.593	Very High
8.	The use of host based controls to improve the security and auditing on endpoints. Such as Intrusion Detection/Prevention System, firewall. etc.	82	4.18	0.877	High
9.	Network devices secure configuration. Such as VLANS, Encryption, Tunnels, password encryption	82	4.38	0.678	Very High
10	Vulnerability assessment and management.	82	3.84	0.808	High
11	The use of perimeter, system, endpoint and mobile devices malware inspection and protection.	82	3.84	0.923	High
12	Encryption of confidential data and information.	82	4.18	0.970	High
13	Application control by whitelisting of application e.g. by using Microsoft Software Restriction Policies.	82	3.82	0.818	High
14	The implementation of a backup and recovery plan within the organization.	82	4.45	0.740	Very High
15	Secure network design using concepts such as segregation, zoning, filtering, monitoring.	82	4.22	0.737	Very High

16	The control of wireless access within the organization.	79	4.16	0.966	High
17	Monitoring and analysis of security audit logs.	82	3.77	0.672	High
18	Controlled administrative privileges for the IT team on the servers and data.	82	4.24	0.825	Very High
19	Data integrity checking.	82	3.35	0.973	Moderate
20	Data loss prevention plan.	82	3.94	0.998	High
21	Having an internal and external penetration testing exercise.	82	4.10	0.840	High
22	Email usage control with email malware and Anti-Spam detection and quarantine.	82	4.28	0.742	Very High
23	Web content filtering of incoming and outgoing traffic.	82	4.15	0.788	High
24	User access control and privileges.	82	4.28	0.672	Very High
25	Encryption for server-to-server and client-to-server communication.	82	4.11	0.846	High
	Total	82	4.12	0.526	High

In light of the above analysis, it can be noticed that the total Mean response for the applied controls was (4.12) out of (5.00), which is considered **High**. Therefore we can say that there is a **High** application degree of information security management controls in Palestinian Banks; that is very good but still need more attention and improvements.

This can be justified due to the fact that there is internal and external audit for information security in the banks. In addition to responsibility of PMA on Palestinian banks.

More details from the table (4-10) we can see that:

- ✓ Controls (2, 7, 9, 14, 15, 18, 22 and 24) were applied in very high degree.

- ✓ Controls (4 and 19) were applied in a moderate degree; this lead that banks should do more effort in training employees and do improve awareness for the employees in dealing with information. In addition to give data integrity checking more importance.
- ✓ Other factors applied in a high degree which mean they need to review and improve.

Section two hypotheses testing:

H₁₀: There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between Palestinian Banks in applying the Information Security Management controls attributed to **Number of the bank's Branches/Offices** variable.

Table (4-11) shows that there is neither positive nor inverse relation between the Number of the bank's Branches/Offices and Information Security Management controls application degree, but it's clear that the banks with 10-19 branches applying a **Very high** degree of Information Security Management controls, while the rest applying High degree of Information Security Management controls.

Table (4-11): Number of the bank's Branches/Offices

Number of the bank Branches/Offices	Frequency	Mean	S.D.	Application Degree
5 branches or less	19	4.08	0.676	High
6 to10 branches	17	4.02	0.436	High
10 to 19 branches	24	4.38	0.442	Very High
20 or more branches	22	3.95	0.445	High
Total	82	4.12	0.526	High

To test the hypothesis the researcher used One-Way ANOVA test:

The results in the table (4-12) show that the significance of applying Information Security Management controls is (0.027) which is less than (0.05); this denotes that there are significant differences between Palestinian Banks in applying Information Security Management controls due to the Number of the bank's Branches/Offices.

Table (4-12): ANOVA test for Number of the Bank's Branches/Offices

Section 2	Sum of Squares	Df	Mean Square	F	Sig.
Current State					
Between Groups	2.479	3	0.826	3.236	0.027
Within Groups	19.922	78	0.255		
Total	22.402	81			

According to these results; we cannot accept the hypothesis "There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between Palestinian Banks in applying the Information Security Management controls attributed to Number of the bank Branches/Offices variable".

In order to get deep investigation, LSD Post Hoc tests used as shown in table (4-13). Therefore it's clear that these differences are in favor of banks' with 10-19 branches.

Table (4-13): LSD Post Hoc Tests for Number of Branches/Offices

(I) Number of Branches	(J) Number of Branches	Mean Difference (I-J)	Std. Error	Sig.
5 branches or less	6 - 10 branches	0.0630	0.16872	0.710
	10 to 19 branches	-0.2966	0.15519	0.060
	20 or more branches	0.1369	0.15828	0.390
6 - 10 branches	5 branches or less	-0.0630	0.16872	0.710
	10 to 19 branches	-0.3597*	0.16021	0.028
	20 or more branches	0.0739	0.16320	0.652
10 to 19 branches	5 branches or less	0.2966	0.15519	0.060
	6 - 10 branches	0.3597*	0.16021	0.028
	20 or more branches	0.4336*	0.14917	0.005
20 or more branches	5 branches or less	-0.1369	0.15828	0.390
	6 - 10 branches	-0.0739	0.16320	0.652
	10 to 19 branches	-0.4336*	0.14917	0.005

*.The mean difference is significant at the .05 level.

H₂₀: There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between Palestinian banks in applying the Information Security

Management controls attributed to holding International Information Security Management standard.

In order to test the hypothesis; descriptive statistics and independent T-test used. Therefore table (4-14) shows that there is a positive correlation between the banks' holding International Information Security Management standard and the application degree of Information Security Management controls. Therefore banks' holding International Information Security Management standard applying **Very high** degree of Information Security Management controls, where others applying **High** degree of Information Security Management controls.

Table (4-14): Banks holding ISM standard

Standard	Frequency	Mean	S.D.	Application Degree
Yes	47	4.30	0.401	Very High
No	34	3.86	0.574	High
Total	81	4.12	0.526	High

To test if this difference is statistically significant ($\alpha \leq 0.05$), independent T-test used, where the result was ($t=3.236$) and ($\text{Sig.} = 0.000$). Therefore we cannot accept the hypothesis "There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between Palestinian Banks in applying the Information Security Management controls attributed to holding International Information Security Management standard.

Returning to Table (4-14) it's clear that these differences are in favor of banks' holding International Information Security Management standard.

4.4.2. Influence of Research Domains on the Effectiveness of ISM

This is the third section of the questionnaire; the output of analyzing this section should answer the research second question, in addition to test research hypotheses that are relevant to the respondents.

Research's Second Question:

What are most influential domains and controls that influence the effectiveness of Information Security Management from the point of respondents of view?

To answer this question; Descriptive statistics used in order to get Means, Standard deviation (S.D.), and application degree for each control, and for all controls.

According to table (4-15) the respondents claim that **People** domain affects in a **Very High** degree (4.29), on the effectiveness of Information Security Management, while they think that control #1 affect with the least degree, comparing to other controls.

Table (4-15): People Effectiveness degree

No.	Domain /Control	N	Mean	S.D.	Effectiveness degree
Domain One: People					
1.	Security and academic checks at the time of recruitment.	81	4.14	0.754	High
2.	Awareness of information security training courses.	82	4.30	0.977	Very High
3.	Logical access control procedure and policy.	82	4.32	0.664	Very High
4.	Information security policy is approved and known by employees.	82	4.41	0.769	Very High
5.	Segregation of duties.	82	4.26	0.829	Very High
	Total	82	4.29	0.604	Very High

From the last table (4-15), the respondents claim that **Process** domain affects in a **High** degree (4.10), on the effectiveness of Information Security Management. In addition they think that control #3 and control #4 affect in a relatively higher degree than other controls.

Table (4-16): Process Effectiveness degree

No.	Domain /Control	N	Mean	S.D.	Effectiveness degree
Domain Two: Process					
1.	Documentation of information security policy.	82	4.04	0.761	High
2.	Change management i.e., any change to be made goes through the change control authorization process.	82	3.91	0.724	High
3.	Documentation of operating procedures.	82	3.93	0.663	High
4.	Including information security in the business continuity management process.	82	4.27	0.704	Very High
5.	Risk assessment and management.	82	4.37	0.694	Very High
	Total	82	4.10	0.488	High

From the last table (4-17), the respondents claim that **Product/ Technology** domain affects in a **High** (4.12), degree on the effectiveness of Information Security Management. In addition they think that control #4 and control #5 affect in a higher degree than other controls.

Table (4-17): Product/ Technology Effectiveness degree

No.	Domain /Control	N	Mean	S.D.	Effectiveness degree
Domain Three: Product/ Technology					
1.	Physical and environmental security management.	82	3.94	0.775	High
2.	Equipment security management.	82	4.09	0.724	High
3.	Access controls management.	82	4.01	0.694	High
4.	Protection against malicious software.	82	4.23	0.725	Very High
5.	Backup and recovery management.	82	4.34	0.724	Very High
	Total	82	4.12	0.609	High

From the last table (4-18), the respondents claim that **Partners/Suppliers** domain affects in a **High** degree (3.97), on the effectiveness of Information Security Management. In addition they think that all controls have almost the same impact.

Table (4-18): Partners/Suppliers Effectiveness degree

No.	Domain /Control	N	Mean	S.D.	Effectiveness degree
Domain Four: Partners/Suppliers					
1.	Addressing security when dealing with customers.	82	3.99	0.778	High
2.	Third party service delivery management.	82	3.85	0.756	High
3.	System acceptance such as new information systems, upgrades and new versions.	82	4.09	0.632	High
4.	Supplier profile and qualification check in addition to service registration and staff qualification certificates.	82	3.95	0.874	High
5.	Define Service level agreement with all suppliers and 3rd parties.	82	3.98	0.666	High
	Total	82	3.97	0.564	High

Table (4-19): Data Effectiveness degree

No.	Domain /Control	N	Mean	S.D.	Effectiveness degree
Domain Five: Data					
1.	Secure data at rest and in motion.	82	4.22	0.770	Very High
2.	Data masking in test and developments environment.	82	3.87	0.813	High
3.	Apply very strong policy and procedures for IT staff specially the DBA when accessing the data.	82	3.98	0.753	High
4.	Sign NDA with the vendors especially when they need to access the data.	82	4.04	0.808	High
5.	Data labeling and handling in accordance with the classification scheme adopted by the organization.	82	3.94	0.791	High
	Total	82	4.01	0.624	High

From the last table (4-19), the respondents think that Data domain affects in a **High** degree (4.01), on the effectiveness of Information Security Management, while they think that control #1 affects in a higher degree than other controls.

According to table (4-20), and depending on domains means, we could arrange the influence of the five domains on the effectiveness of Information Security Management. Therefore respondents claim that “People” are considered the dominant domain that influences the effectiveness of Information Security Management with a very high degree.

Table (4-20): Section Three Effectiveness degree

No.	Domain	N	Mean	Standard Deviation	Effectiveness degree
1.	Domain One: People	82	4.29	0.604	Very High
2.	Domain Two: Process	82	4.10	0.488	High
3.	Domain Three: Product/ Technology	82	4.12	0.609	High
4.	Domain Four: Partners/Suppliers	82	3.97	0.564	High
5.	Domain Five: Data	82	4.01	0.624	High
	Total	82	4.10	0.452	High

This result could be justified; therefore as long as using all restricted process and top technology, security can't be achieved without the human collaboration and people awareness.

Gelbstein (2013) agrees this result, he claims that “people at all levels of the organisation are the weakest element of information security. In addition people play a major role in information security activities”.

Section three hypotheses:

H₃₀: There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between research's domains that influence the Effectiveness of Information Security Management in Palestinian Banks from the point of respondents' view, attributed to respondents' **Qualification** variable.

Table (4-21) explores the differences of respondents' opinion about the influence of research domains on the effectiveness of Information Security Management according to their qualifications:

Table (4-21): Section three & Qualification statistics

Section3	Qualification	N	Mean	S.D.	Effectiveness Degree
Domain 1 People	Diploma or less	3	3.47	0.115	High
	Bachelor	61	4.32	0.597	Very High
	High Education	18	4.30	0.595	Very High
	Total	82	4.29	0.604	Very High
Domain 2 Processes	Diploma or less	3	3.93	0.503	High
	Bachelor	61	4.13	0.494	High
	High Education	18	4.04	0.483	High
	Total	82	4.10	0.488	High
Domain 3 Products/ Technology	Diploma or less	3	4.47	0.503	Very High
	Bachelor	61	4.10	0.614	High
	High Education	18	4.14	0.620	High
	Total	82	4.12	0.609	High
Domain 4 Partners/ Suppliers	Diploma or less	3	3.93	0.416	High
	Bachelor	61	3.97	0.598	High
	High Education	18	3.97	0.481	High
	Total	82	3.97	0.564	High
Domain 5 Data	Diploma or less	3	4.47	0.611	Very High
	Bachelor	61	3.99	0.611	High
	High Education	18	3.98	0.675	High
	Total	82	4.01	0.624	High
Section Three Total	Diploma or less	3	4.05	0.420	High
	Bachelor	61	4.10	0.465	High
	High Education	18	4.09	0.433	High
	Total	82	4.10	0.452	High

- ✓ **People domain:** Respondents with diploma or less "qualification claim that "People" influence in High degree, while others claim that "People" influence in Very High degree.
- ✓ **Processes domain:** Respondents regardless to qualification claim that "Processes" influence in High degree.
- ✓ **Products/Technology domain:** Respondents with diploma or less qualification claim that "Products/Technology" influence in Very High degree, while others claim that "Products/Technology" influence in High degree.
- ✓ **Partners/Suppliers domain:** Respondents regardless to qualification claim that "Partners/Suppliers" influence in High degree.
- ✓ **Data domain:** Respondents with diploma or less qualification claim that "Data" influence in Very High degree, while others claim that "Data" influence in High degree.

In order to test the hypothesis One-Way ANOVA used. Therefore table (4-22) shows that significant probability for all domains and for total degree is more than (0.05), thus we cannot reject the null hypothesis. "There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between research domains that influence the effectiveness of Information Security Management in Palestinian Banks from the point of respondents view, attributed to respondents **Qualification** variable".

Table (4-22): ANOVA test for Qualification

Section3	Source of Variance	Sum of Squares	df	Mean Square	F	Sig.
Domain 1 People	Between Groups	2.093	2	1.047	3.015	0.055
	Within Groups	27.429	79	0.347		
	Total	29.522	81			
Domain 2 Processes	Between Groups	0.186	2	0.093	0.384	0.682
	Within Groups	19.114	79	0.242		
	Total	19.300	81			
Domain 3 Products/ Technology	Between Groups	0.400	2	0.200	0.532	0.589
	Within Groups	29.661	79	0.375		
	Total	30.060	81			
Domain 4 Partners/ Suppliers	Between Groups	0.005	2	0.003	0.008	0.992
	Within Groups	25.765	79	0.326		
	Total	25.770	81			
Domain 5 Data	Between Groups	0.660	2	0.330	0.844	0.434
	Within Groups	30.895	79	0.391		
	Total	31.556	81			
Section Three Total	Between Groups	0.010	2	0.005	0.023	0.977
	Within Groups	16.541	79	0.209		
	Total	16.551	81			

H4₀: There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between research's domains that influence the effectiveness of Information Security Management in Palestinian Banks from the point of respondents view, attributed to respondents' **Specialty** variable.

Table (4-23) explores the differences of respondents' opinion about the influence of research domains on the effectiveness of Information Security Management according to their **Specialty** variable.

Table (4-23): Section three & Specialty statistics

Section3	Specialty	N	Mean	S.D.	Effectiveness Degree
Domain 1 People	Administration	16	4.36	0.646	Very High
	Engineering	19	4.09	0.620	High
	IT	46	4.34	0.584	Very High
	Total	81	4.29	0.607	Very High
Domain 2 Processes	Administration	16	3.93	0.467	High
	Engineering	19	3.96	0.474	High
	IT	46	4.22	0.481	Very High
	Total	81	4.10	0.491	High
Domain 3 Products/ Technology	Administration	16	4.06	0.664	High
	Engineering	19	3.82	0.565	High
	IT	46	4.27	0.572	Very High
	Total	81	4.13	0.612	High
Domain 4 Partners/ Suppliers	Administration	16	3.94	0.504	High
	Engineering	19	3.99	0.514	High
	IT	46	3.98	0.615	High
	Total	81	3.98	0.566	High
Domain 5 Data	Administration	16	3.86	0.786	High
	Engineering	19	4.03	0.654	High
	IT	46	4.05	0.561	High
	Total	81	4.01	0.628	High
Section Three Total	Administration	16	4.03	0.532	High
	Engineering	19	3.98	0.427	High
	IT	46	4.17	0.431	High
	Total	81	4.10	0.454	High

- ✓ People domain: Respondents with administration and IT Specialty claim that “People” influence in Very High degree, while engineers claim that “People” influence in High degree.
- ✓ Processes domain: Respondents with IT Specialty claim that “Processes” influence in Very High degree, while all others claim that “Processes” influence in High degree.
- ✓ Products/Technology domain: Respondents with IT Specialty claim that “Products/Technology” influence in Very High degree, while all others claim that “Products/Technology” influence in High degree.
- ✓ Partners/Suppliers domain: Respondents regardless to qualification claim that “Partners/Suppliers” influence in High degree.
- ✓ Data domain: Respondents regardless to qualification claim that “Data” influence in High degree.

In order to test the hypothesis One-Way ANOVA used. Therefore table (4-24) shows that significant probability for domain three “Products/Technology” is (0.044) which less than (0.05), thus we cannot accept H_0 for this domain.

Table (4-24): ANOVA test for Specialty

Section3	Source of Variance	Sum of Squares	df	Mean Square	F	Sig.
Domain 1 People	Between Groups	0.940	2	0.470	1.286	0.282
	Within Groups	28.500	78	0.365		
	Total	29.440	80			
Domain 2 Processes	Between Groups	1.555	2	0.778	3.420	0.038
	Within Groups	17.735	78	0.227		
	Total	19.290	80			
Domain 3 Products/ Technology	Between Groups	2.838	2	1.419	4.081	0.021
	Within Groups	27.118	78	0.348		
	Total	29.956	80			
Domain 4 Partners/ Suppliers	Between Groups	0.029	2	0.015	0.044	0.957
	Within Groups	25.601	78	0.328		
	Total	25.631	80			
Domain 5 Data	Between Groups	0.422	2	0.211	0.529	0.591
	Within Groups	31.133	78	0.399		
	Total	31.556	80			
Section three Total	Between Groups	0.608	2	0.304	1.491	0.232
	Within Groups	15.911	78	0.204		
	Total	16.519	80			

Returning back to table (4-24) it's clear that all domains (except domains Two and three) and total degree significant probability was more than (0.05), thus we cannot reject the null hypothesis for these domains and total degree. "There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between research's domains that influence the Effectiveness of Information Security Management in Palestinian Banks from the point of respondents view, attributed to respondents **Specialty** variable".

In order to get deep investigation, LSD Post Hoc tests used as shown in table (4-25). Therefore it's clear that these differences are in favor of IT specialty.

Table (4-25): LSD Post Hoc Tests for Specialty

Section3	(I) Number of Branches	(J) Number Of Branches	Mean Difference (I-J)	Std. Error	Sig.
Domain 1 People	Administration	Engineering	0.2678	0.2051	0.1956
		IT	0.0190	0.1754	0.9139
	Engineering	Administration	-0.2678	0.2051	0.1956
		IT	-0.2487	0.1648	0.1354
	IT	Administration	-0.0190	0.1754	0.9139
		Engineering	0.2487	0.1648	0.1354
Domain 2 Processes	Administration	Engineering	-0.0329	0.1618	0.8394
		IT*	-0.2967	0.1384	0.0351
	Engineering	Administration	0.0329	0.1618	0.8394
		IT*	-0.2638	0.1300	0.0459
	IT	Administration *	0.2967	0.1384	0.0351
		Engineering*	0.2638	0.1300	0.0459
Domain 3 Products/ Technology	Administration	Engineering	0.2414	0.2001	0.2311
		IT	-0.2114	0.1711	0.2204
	Engineering	Administration	-0.2414	0.2001	0.2311
		IT*	-0.4529	0.1608	0.0061
	IT	Administration	0.2114	0.1711	0.2204
		Engineering*	0.4529	0.1608	0.0061
Domain 4 Partners/ Suppliers	Administration	Engineering	-0.0520	0.1944	0.7899
		IT	-0.0451	0.1663	0.7869
	Engineering	Administration	0.0520	0.1944	0.7899
		IT	0.0069	0.1562	0.9651
	IT	Administration	0.0451	0.1663	0.7869
		Engineering	-0.0069	0.1562	0.9651
Domain 5 Data	Administration	Engineering	-0.1691	0.2144	0.4327
		IT	-0.1853	0.1834	0.3153
	Engineering	Administration	0.1691	0.2144	0.4327
		IT	-0.0162	0.1723	0.9251

	IT	Administration	0.1853	0.1834	0.3153
		Engineering	0.0162	0.1723	0.9251
Section three Total	Administration	Engineering	0.0511	0.1532	0.7399
		IT	-0.1439	0.1311	0.2756
	Engineering	Administration	-0.0511	0.1532	0.7399
		IT	-0.1950	0.1232	0.1175
	IT	Administration	0.1439	0.1311	0.2756
		Engineering	0.1950	0.1232	0.1175

*.The mean difference is significant at the .05 level.

H5₀: There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between research's domains that influence the Effectiveness of Information Security Management in Palestinian Banks from the point of respondents view, attributed to respondents **Experience** variable.

According to table (4-26), we can explore the differences of respondents' opinion about the influence of research domains on the effectiveness of Information Security Management according to their **Experience** variable.

Table (4-26): Section three & Experience statistics

Section3	Experience	N	Mean	S.D.	Effectiveness Degree
Domain 1 People	5 years or less	15	4.13	0.708	High
	6 - 10 years	22	4.20	0.589	High
	11 - 15 years	25	4.37	0.457	Very High
	More than 15 years	20	4.39	0.700	Very High
	Total	82	4.29	0.604	Very High
Domain 2 Processes	5 years or less	15	4.11	0.604	High
	6 - 10 years	22	4.14	0.529	High
	11 - 15 years	25	4.12	0.451	High
	More than 15 years	20	4.04	0.419	High
	Total	82	4.10	0.488	High
Domain 3 Products/ Technology	5 years or less	15	4.28	0.512	Very High
	6 - 10 years	22	4.13	0.628	High
	11 - 15 years	25	4.05	0.672	High
	More than 15 years	20	4.09	0.596	High
	Total	82	4.12	0.609	High
Domain 4 Partners/ Suppliers	5 years or less	15	4.15	0.444	High
	6 - 10 years	22	3.90	0.632	High
	11 - 15 years	25	3.90	0.530	High
	More than 15 years	20	4.00	0.616	High
	Total	82	3.97	0.564	High
Domain 5 Data	5 years or less	15	4.19	0.463	High
	6 - 10 years	22	4.05	0.676	High
	11 - 15 years	25	3.84	0.572	High
	More than 15 years	20	4.04	0.721	High
	Total	82	4.01	0.624	High
Section Three Total	5 years or less	15	4.17	0.455	High
	6 - 10 years	22	4.08	0.492	High
	11 - 15 years	25	4.06	0.409	High
	More than 15 years	20	4.11	0.483	High
	Total	82	4.10	0.452	High

- ✓ People domain: Respondents with ten or less years' Experience claim that "People" influence in High degree, while others claim that "People" influence in Very High degree.
- ✓ Processes domain: Respondents regardless to Experience claim that "Processes" influence in High degree.
- ✓ Products/Technology domain: Respondents with five or less years' Experience claim that "Products/Technology" influence in Very High degree, while others claim that "Products/Technology" influence in High degree.
- ✓ Partners/Suppliers domain: Respondents regardless to Experience claim that "Partners/Suppliers" influence in High degree.
- ✓ Data domain: Respondents regardless to Experience claim that "Data" influence in High degree.

In order to test the hypothesis One-Way ANOVA used. Therefore table (4-27) shows that significant probability for all domains and for total degree is more than (0.05), thus we cannot reject the null hypothesis. "There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between research's domains that influence the Effectiveness of Information Security Management in Palestinian Banks from the point of respondents view, attributed to respondents **Experience** variable".

Table (4-27): ANOVA test for Experience

Section3	Source of Variance	Sum of Squares	df	Mean Square	F	Sig.
Domain 1 People	Between Groups	0.897	3	0.299	0.814	0.490
	Within Groups	28.626	78	0.367		
	Total	29.522	81			
Domain 2 Processes	Between Groups	0.111	3	0.037	0.151	0.929
	Within Groups	19.188	78	0.246		
	Total	19.300	81			
Domain 3 Products/ Technology	Between Groups	0.532	3	0.177	0.469	0.705
	Within Groups	29.528	78	0.379		
	Total	30.060	81			
Domain 4 Partners/ Suppliers	Between Groups	0.703	3	0.234	0.729	0.538
	Within Groups	25.067	78	0.321		
	Total	25.770	81			
Domain 5 Data	Between Groups	1.236	3	0.412	1.060	0.371
	Within Groups	30.320	78	0.389		
	Total	31.556	81			
Section three Total	Between Groups	0.133	3	0.044	0.211	0.889
	Within Groups	16.418	78	0.210		
	Total	16.551	81			

H₀: There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between research's domains that influence the Effectiveness of Information Security Management in Palestinian Banks from the point of respondents view, attributed to respondent's IS **certifications** variable.

Table (4-28) shows that significant probability for domain one (0.004) which is less than (0.05), thus we cannot accept H₀ for this domain, and returning to the same table, it's clear that these differences are in favor of whom carrying certifications related to information security, but domains

2,3,4,5 and total degree it was more than (0.05), thus we cannot reject the null hypothesis for these domains and total degree. “There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between research’s domains that influence the Effectiveness of Information Security Management in Palestinian Banks from the point of respondents view, attributed to respondents **IS certifications** variable”.

Table (4-28): t- test for Experience

Section3	IS Cert.	N	Mean	S.D.	Effectiveness degree	t	Sig.
Domain 1 People	Yes	26	4.56	0.427	Very High	2.954	0.004
	No	56	4.16	0.633	High		
Domain 2 Processes	Yes	26	4.22	0.379	Very High	1.437	0.155
	No	56	4.05	0.526	High		
Domain 3 Products/ Technology	Yes	26	4.08	0.709	High	-0.376	0.708
	No	56	4.14	0.563	High		
Domain 4 Partners/ Suppliers	Yes	26	4.01	0.444	High	0.402	0.689
	No	56	3.95	0.615	High		
Domain 5 Data	Yes	26	4.14	0.571	High	1.302	0.197
	No	56	3.95	0.643	High		
Section Three Total	Yes	26	4.20	0.369	Very High	1.428	0.157
	No	56	4.05	0.481	High		

H7₀: There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between research's domains that influence the effectiveness of Information Security Management in Palestinian Banks from the point of respondents view, attributed to respondent's **work field** variable.

Table (4-29) explores the differences of respondents' opinion about the influence of research domains on the effectiveness of Information Security Management according to their **Work Field** variable.

Table (4-29): Section three & Work Field statistics

Section3	Work Field	N	Mean	S.D.	Effectiveness Degree
Domain 1 People	Administrative	33	4.39	0.596	Very High
	Technical	43	4.23	0.601	Very High
	Both	6	4.13	0.689	High
	Total	82	4.29	0.604	Very High
Domain 2 Processes	Administrative	33	4.07	0.486	High
	Technical	43	4.13	0.486	High
	Both	6	4.13	0.589	High
	Total	82	4.10	0.488	High
Domain 3 Products/ Technology	Administrative	33	4.13	0.646	High
	Technical	43	4.08	0.604	High
	Both	6	4.33	0.468	Very High
	Total	82	4.12	0.609	High
Domain 4 Partners/ Suppliers	Administrative	33	4.03	0.548	High
	Technical	43	3.93	0.589	High
	Both	6	3.97	0.528	High
	Total	82	3.97	0.564	High
Domain 5 Data	Administrative	33	4.03	0.716	High
	Technical	43	3.98	0.575	High
	Both	6	4.07	0.484	High
	Total	82	4.01	0.624	High
Section Three Total	Administrative	33	4.13	0.497	High
	Technical	43	4.07	0.419	High
	Both	6	4.13	0.488	High
	Total	82	4.10	0.452	High

- ✓ People domain: Respondents in administrative and technical Work Field claim that “People” influence in Very High degree, while Respondents combine both Work Field claim that “People” influence in High degree.
- ✓ Processes domain: Respondents regardless to Work Field claim that “Processes” influence in High degree.
- ✓ Products/Technology domain: Respondents in administrative and technical Work Field claim that “Products/Technology” influence in High degree, while Respondents combine both Work Fields claim that “Products/Technology” influence in Very High degree.
- ✓ Partners/Suppliers domain: Respondents regardless to Work Field claim that “Partners/Suppliers” influence in High degree.
- ✓ Data domain: Respondents regardless to Work Field claim that “Data” influence in High degree.

In order to test the hypothesis One-Way ANOVA used. Therefore; table (4-30) shows that significant probability for all domains and for total degree is more than (0.05), thus we cannot reject the null hypothesis. “There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between research’s domains that influence the effectiveness of Information Security Management in Palestinian banks from the point of respondents view, attributed to respondents **work field** variable”.

Table (4-30): ANOVA test for Work Field

Section3	Source of Variance	Sum of Squares	df	Mean Square	F	Sig.
Domain 1 People	Between Groups	0.627	2	0.314	0.858	0.428
	Within Groups	28.895	79	0.366		
	Total	29.522	81			
Domain 2 Processes	Between Groups	0.071	2	0.035	0.146	0.865
	Within Groups	19.229	79	0.243		
	Total	19.300	81			
Domain 3 Products/ Technology	Between Groups	0.335	2	0.168	0.445	0.642
	Within Groups	29.725	79	0.376		
	Total	30.060	81			
Domain 4 Partners/ Suppliers	Between Groups	0.205	2	0.102	0.317	0.730
	Within Groups	25.565	79	0.324		
	Total	25.770	81			
Domain 5 Data	Between Groups	0.067	2	0.034	0.085	0.919
	Within Groups	31.488	79	0.399		
	Total	31.556	81			
Section three Total	Between Groups	0.075	2	0.037	0.179	0.836
	Within Groups	16.476	79	0.209		
	Total	16.551	81			

4.5. Discussion

It appears clearly that the status of information security management in Palestinian Banks applied in high degree, however there is variance between controls applied. In addition; the application degree differences attributed to Number of the bank Branches/Offices variable and whether the bank holding International Information Security Management standard.

✓ **First research question:**

“To what extent do research controls applied in Palestinian banks to achieve Information Security Management?”

According to table (4-10), it's clear that total Mean response for the applied controls is (82.4%), which considered **high**. Therefore we can say that there is a **High** application degree of information security management controls in Palestinian banks.

Palestinian banks need more efforts in applying some controls such as “Users training & awareness e.g. Internet threats, spear phishing socially engineered email”, and “Data integrity checking”, these controls were discussed earlier in literature review and they are very important.

According to “Training and awareness” Tayeh (2008), in the study “Effectiveness of Information Security Management at the Palestinian Information Technology Companies”, found that less than one half of companies (41.4%) conducting training in the information security for all employees, and regularly updating they about organizational policies and procedures, while around one third (29.2%) of them do not conduct such that training.

But according to “Data Integrity”, on contrast (Tayeh, 2008) found that high majority of companies (92.5%) applying some controls to protect the integrity of publicly available information from any unauthorized access, while other companies (7.5%) do not apply such kind of controls.

It is clearly obvious that Palestinian banks need to include information security management in strategic planning. In addition to increase the training and awareness for the employees to information security.

✓ **Second research question:**

It appears clearly that the most dominant domains influencing information security management are people, technology and process. Followed by data and partners/ suppliers, which is compatible with (Posthumus & Von Solms, 2004).

Regarding to table (4-30), the results show that the maximum mean (4.29) refers to the “People” domain, which is a justified and reasonable result .On contrast, the minimum mean value (3.97) refers to partner or supplier attribute.

Table (4-31): Research domains Effectiveness degree

No.	Domain	N	Mean	Standard Deviation	Effectiveness degree
1.	Domain One: People	82	4.29	0.604	Very High
2.	Domain Two: Process	82	4.10	0.488	High
3.	Domain Three: Product/ Technology	82	4.12	0.609	High
4.	Domain Four: Partners/Suppliers	82	3.97	0.564	High
5.	Domain Five: Data	82	4.01	0.624	High
	Total	82	4.10	0.452	High

Werlinger et al. (2009) used empirical data and prior work to provide an integrated view of the various human, organizational, and technological

challenges that security experts face within their organizations. In addition he classified three challenges as human factors into, Lack of security training, lack of a security culture; and communication of security issues.

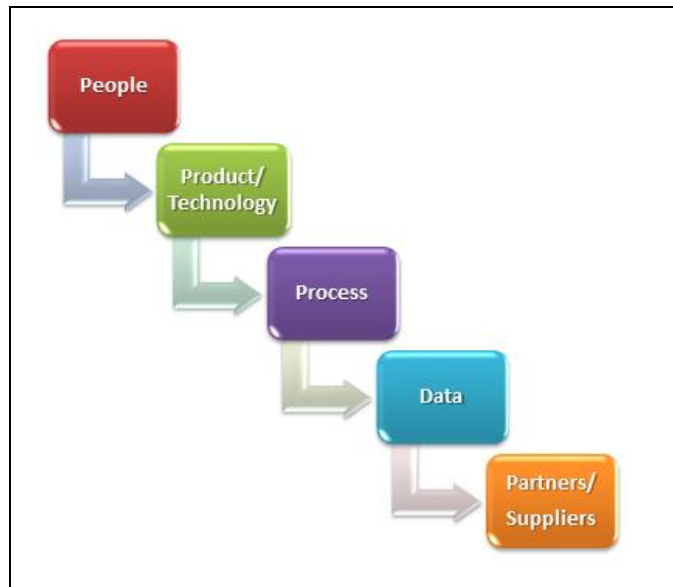


Figure (4-1): Rank of the five domains depending on the means

Silic and Back (2013) define Information Security Management as “a systematic approach to encompassing people, processes, and Information Technology (IT) systems that safeguards critical systems and information, protecting them from internal and external threats”.

Technology is very important in protecting data. However, technology comes with a high price tag. Therefore with IT budgets being chipped away in the name of cost savings, technology solutions are usually the first to be eliminated (Rashidi et al., 2011).

While technology is an absolute necessary in our high tech, web-centric world, is not the be-all and end-all when it comes to computer security. It

certainly is critical to have secure firewalls, intrusion detection systems, spam guards, etc. However, all the network security in the world isn't going to keep networks safe if employees are not properly trained.

The need for having open and secure networks had an influence on the interactions between participants and security vendors; it can be difficult for vendors to understand the architecture of the network and offer products that suit the organization's needs(Werlinger et al., 2009).

According to a study done by Stellar et al. (2012), Information Systems Ltd, human error is the single largest contributor to incidents of data loss and corruption. These errors include, but are not limited to: accidental drive format, erroneous file/folder deletion, MIS/administrator errors, and mishandling of data.

The results can be devastating to a network. There is also a growing mobile workforce, which brings its own unique set of security hazards. Unencrypted USB drives, laptops, PDAs and other devices are also an increasing threat to information security(It et al., 2011).

Hypotheses discussion with related studies:

H1₀: There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between Palestinian Banks in applying the Information Security Management controls attributed to **Number of the bank's Branches/Offices** variable.

- ✓ Kankanhalli et al. (2003), Small and medium-sized enterprises were found to engage in fewer deterrent efforts compared to larger organizations. Financial organizations were found to undertake more deterrent efforts and have stiffer deterrent severity than organizations in other sectors.
- ✓ S. E. Chang and Ho (2006), there were significant impacts of organizational factors, including IT competence of business managers, environment uncertainty, industry type, and organization size, on the effectiveness of implementing Information Security Management.

H2₀: There are no differences denoting a statistical significance ($\alpha \leq 0.05$) between Palestinian Banks in applying the Information Security Management controls attributed to **holding International ISM standard** variable.

- ✓ R. Von Solms (1999), an IT-environment should utilize a technically secure computer base, preferably evaluated by TCSEC or ITSEC. This computer base should be operated in a secure way and evaluated and certified as doing just that. All of this can only be accomplished through adequate information security standards. Standards like TCSEC and ITSEC, GMITS and BS7799 can certainly provide the basis to ensure "safe driving on the information super highway".

- ✓ M. Siponen and Willison (2009), international information security management guidelines play a key role in managing and certifying organizational Information Systems. Although they don't pay enough attention to the differences between organizations and the fact that their security requirements are different. Second, these guidelines were validated by appeal to common practice and authority and that this was not a sound basis for important international information security guidelines.

Conclusion

This section outlines the statistical difference between participants in this research. Independent Samples Test (t-test for Equality of Means) for two levels variables. In addition one-way ANOVA Test for more than two levels variables are used to explain these differences. Therefore these two tests are used to highlight whether the means of several variables are equal or not.

When significant differences were found descriptive statistics and another Post-hoc test (LSD) was conducted to understand the differences between the surveyed banks due to the specific independent variable.

The results of section two show that there is a moderate application degree in “Training and awareness” controls. In addition the results of section three show that respondents claim that “People” is the most influential domain on the effectiveness of Information Security Management. Therefore Palestinian banks should take this result in consideration.

Chapter Five

Conclusions and Recommendations

5. Conclusions and Recommendations

This chapter will briefly overview the research results, and explores recommendations that are based on the research findings in order to identification of the current state of Information Security Management practices in Palestinian banking sector. However to exploring the influencing factors surrounding the effectiveness of Information Security Management practices. In addition, this chapter will present the research contribution to current literature and the suggestions of conducting future studies.

5.1. Overview

This thesis addressed the status of Information Security Management in Palestinian banking, as well as the factors that influence the effectiveness of Information Security Management process. Furthermore, it highlights the importance of information security.

Thesis indicated a lot of Information Security Management best practices. Moreover, it defines the information security and corporate governance, and discusses the main domain influence the effectiveness of Information Security Management.

The main finding of this research that information security is not abstract process and technology, training and awareness of people is more important in addition to the rest controls.

However information security is not technical issue, but it should be pillar of strategic decision of any organization and this is compatible with B. von Solms and von Solms (2004) “realizing that information security as a business issue and not a technical issue”.

5.2. Research Contribution

The findings of this research project constitute a basis for Palestinian banks to perform their information security management, where the whole information security management process and factors influencing the effectiveness of information security management were identified.

Palestinian banks can utilize this study to structure their information security management assessment and identify major gaps in their current performance which can be mitigated.

Moreover, researchers can utilize this research as a starting point for further research projects that approaches different aspects of the subject, since the subject was not targeted by other researchers before.

The results of this research are of great importance to researchers, Palestinian banks, and PMA. Therefore, this research is considered to be a significant contribution in Information Security Management, these contributions are:

- ✓ Gives a clear assessment for Information Security Management in Palestinian banks.
- ✓ Measure the current status on Information Security Management in Palestinian banks.
- ✓ Determine factors influencing the effectiveness of Information Security Management.
- ✓ Help Palestinian banks in formulating the right strategies which will make Information Security Management effective.

Following are results founded as the outcome of this thesis:

- ✓ People affecting the effectiveness of Information Security Management in very high degree (85.8%). Therefore employees need more information security training and awareness.
- ✓ Product and technology affecting the effectiveness of Information Security Management in high degree (82.4%). Therefore vulnerability assessment and management should be done. In addition to use of perimeter, system, endpoint and mobile devices malware inspection and protection.
- ✓ Process affecting the effectiveness of Information Security Management in high degree (82.0%). Therefore application control by whitelisting of application should be improved.

- ✓ Partners and suppliers affecting the effectiveness of Information Security Management in high degree (80.2%). Therefore banks must sign NDA with the vendors especially when they need to access the data.
- ✓ Data affecting the effectiveness of Information Security Management in high degree (79.4%). Therefore data integrity checking must be reviewed and activated.
- ✓ There are differences denoting a statistical significance between Palestinian banks in applying Information Security Management controls due to number of bank's branches and whether the bank holding international Information Security Management standards.

The researcher supplemented additional domain "Data" to the 4Ps framework (People, Process, Product/Technology, Partner/ Supplier) that was developed by Information Technology Infrastructure Library (ITIL) (Clinch, 2009). Therefore this could be starting point for developing new Information Security Management framework in future studies.

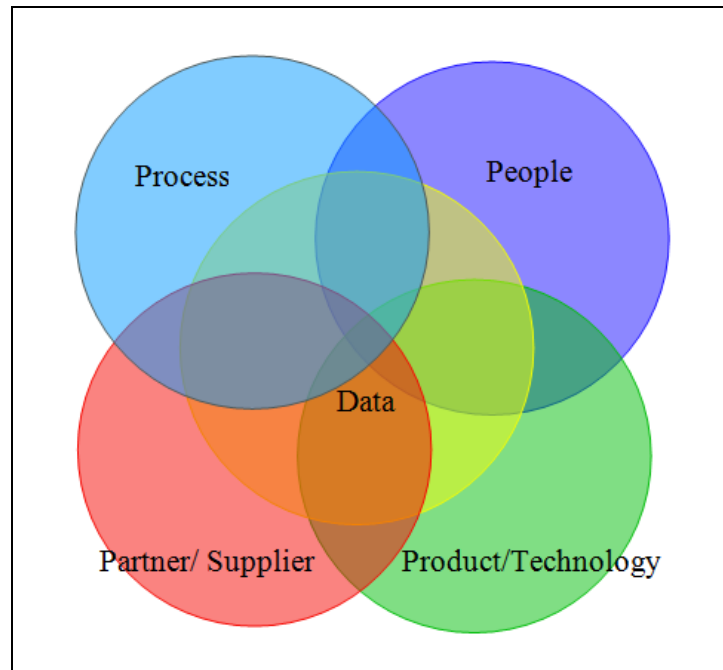


Figure (5-1): Research domains.

5.3. Recommendations

From above discussion and analyze the using information security management in Palestinian banks, and the factors that influence the effectiveness of information security management process, the following recommendations are suggested to be considered:

- ✓ It is recommended to work on changing employees' culture toward information security by management. As long as one of the main findings of this thesis was Palestinian banks didn't pay a lot of attention on awareness, although a "People" is the most important factor influencing the effectiveness of Information security management. Therefore more effort should be done on this arena.
- ✓ Palestinian banks are advised to enhance their practicing of Personnel Security specially the employees training, finding a formal

reporting procedure to report security weaknesses and incidents, and to find a mechanism for quantifying the volume and cost of incidents.

- ✓ Palestinian banks are advised to spend a lot of efforts toward the data integrity checking. Data integrity and validation wasn't efficiently managed by banks; therefore Palestine banks are advised to include data integrity checking in their information security management plan.
- ✓ Palestinian banks are advised to give more concern to the Information Security Management field by following one of the international standards like ISO 27000, ITIL and PCI-DDS.
- ✓ Palestinian banks should concentrate on the long term benefits of information security and do not pressure for short term payoffs.
- ✓ Palestinian banks should improve organizational structure to best suit communication about information security.
- ✓ Palestinian banks should be more aware of their core technical competencies; therefore their information security must be structured based on their overall competitive strategy.
- ✓ Palestinian banks must adopt a more formal and structured approach to information security planning.

- ✓ Palestinian banks should develop their own technology strategy as a means to incorporate information security in the overall business strategy. Therefore acquisition process of any product should address information security as crucial part and aspect of any product or project.
- ✓ Palestinian banks should monitor technology emergence in order to reduce their vulnerability to technological change.
- ✓ Customer feedback should be incorporated while performing information security planning.
- ✓ Palestinian banks should select the right IT security approach that best aligned with its business and financial objects and gives it a competitive advantage. IT security approach should be implemented in a cost efficient manner.
- ✓ Palestinian Government is advised to prepare Palestinian act that organizing the Information Security field; such act should address the information security crimes and its sanctions. Since implementing one of Information security standards such as ISO 27001 may be expensive, it will be a great advantage if the Palestinian standards organization develops a Palestinian information security standard that can cope with information security challenges and best fit Palestinian organization needs.

- ✓ Top management should be educated on information security importance and its crucial impact. Top management should be part of any IT security strategic planning since they should enforce policies and afford financial and human resources.

The empirical investigation suggests that human factor plays an essential role in maintaining information security, and banks can improve employees' role by keeping their security policies up to date and find the best ways to disseminate that information, Therefore it becomes clear that an organization's top security assets are well trained employees rather than state-of-the-art technology.

5.4. Future Studies

The following topics could be studied in the future, which may contribute in performance in Palestine:

- ✓ Study the other factors that affect the performance Information Security Management in Palestinian banks.
- ✓ Study the possibility of developing Palestinian standard for information security management.
- ✓ Study the Role of PMA, Ministry of telecommunications and information technology, and the government in improving and encouraging Information security management in Palestine.

References

- Abu-Musa, A. (2010). **Information security governance in Saudi organizations: an empirical study.** *Information Management & Computer Security*, 18(4), 226-276.
- Adams, S. (2009). *ITIL V3 foundation handbook* (Vol. 1): The Stationery Office.
- Al-Awadi, M. (2009). *A study of employees' attitudes towards organisational information security policies in the UK and Oman.* University of Glasgow.
- Al-Mayahi, I. H., & Sa'ad, P. M. (2014). **Information Security Policy Development.** *Journal of Advanced Management Science* Vol, 2(2).
- Albrechtsen, E. (2004). **Information managed securely? An approach to the social construction of information security management.**
- Albrechtsen, E. (2007). **A qualitative study of users' view on information security.** *Computers & Security*, 26(4), 276-289. doi: 10.1016/j.cose.2006.11.004
- Bacik, S. (2011). Productivity vs. Security. *Information security management handbook*, 5, 429.
- Baker, W. H., & Wallace, L. (2007). **Is information security under control?: Investigating quality in information security management.** *Security & Privacy, IEEE*, 5(1), 36-44.

- Bang, Y., Lee, D.-J., Bae, Y.-S., & Ahn, J.-H. (2012). **Improving information security management: An analysis of ID–password usage and a new login vulnerability measure.** *International Journal of Information Management*, 32(5), 409-418. doi: 10.1016/j.ijinfomgt.2012.01.001
- Bauer, S. (2012). *A Literature Review on Operational IT Risks and Regulations of Institutions in the Financial Service Sector.* Paper presented at the International Conference on Information Resource Management, Vienna. The University of Auckland and WU Vienna.
- Besnard, D., & Arief, B. (2004). **Computer security impaired by legitimate users.** *Computers & Security*, 23(3), 253-264.
- Birgisson, A., Russo, A., & Sabelfeld, A. (2011). **Unifying facets of information integrity.** *Information Systems Security* (pp. 48-65): Springer.
- Bishop, M. (2012). *Computer security: art and science* (Vol. 200): Addison-Wesley.
- Bishop, M., & Taylor, C. (2009). *A Critical Analysis of the Centers of Academic Excellence Program.* Paper presented at the Proceedings of the 13th Colloquium for Information Systems Security Education, Seattle, WA June.
- Bit9. (2014). 2013 Cyber Security Study. 2014, from <http://www.inforisktoday.com/handbooks/2013-cyber-security-study-h->

[46?webSyncID=ed80d890-89d1-3786-eea7-117e83c6bd72&sessionGUID=1827e7a2-540d-eb9d-a8ae-1497e3e031d0](#)

- Blasco, J., Hernandez-Castro, J. C., Tapiador, J. E., & Ribagorda, A. (2012). **Bypassing information leakage protection with trusted applications.** *Computers & Security*, 31(4), 557-568.
- Boehmer, W. (2008). *Appraisal of the effectiveness and efficiency of an Information Security Management System based on ISO 27001*. Paper presented at the Emerging Security Information, Systems and Technologies, 2008. SECURWARE'08. Second International Conference on.
- Breier, J., & Hudec, L. (2013). **On identifying proper security mechanisms** *Information and Communication Technology* (pp. 285-294): Springer.
- Brown, S. (2011). **Characteristics of Effective Security Governance.** *International Journal of Governance*, 1(3), 649-663.
- Bruce, R., Dynes, S., Brechbuhl, H., Brown, B., Goetz, E., Verhoest, P., . . . Helmus, S. (2005). **International policy framework for protecting critical information infrastructure: A discussion paper outlining key policy issues.** *TNO Report, Tuck School of Business at DARMOUTH*.

- Buchanan, S., & Gibb, F. (1998). **The information audit: an integrated strategic approach.** *International Journal of Information Management*, 18(1), 29-47.
- Caralli, R. A., Stevens, J. F., Willke, B. J., & Wilson, W. R. (2004). **The critical success factor method: establishing a foundation for enterprise security management: DTIC Document.**
- Castells, M. (2011). *The rise of the network society: The information age: Economy, society, and culture* (Vol. 1): John Wiley & Sons.
- Chang, K.-c., & Wang, C.-p. (2011). **Information systems resources and information security.** *Information Systems Frontiers*, 13(4), 579-593.
- Chang, S. E., & Ho, C. B. (2006). **Organizational factors to the effectiveness of implementing information security management.** *Industrial Management & Data Systems*, 106(3), 345-361.
- Choobineh, J., Dhillon, G., Grimaila, M. R., & Rees, J. (2007). **Management of information security: challenges and research directions.** *Communications of the Association for Information Systems*, 20(1), 57.
- Clinch, J. (2009). **ITIL V3 and Information Security.** *Best Management Practice., ITIL.*
- Commission, C. o. S. O. o. t. T. (2013). *Internal Control, Integrated Framework.*

- Conner, F. W., & Coviello, A. W. (2004). **Information security governance: a call to action**. *Corporate Governance Task Force Report of 2004*.
- Corpuz, M., & Barnes, P. H. (2010). **Integrating information security policy management with corporate risk management for strategic alignment**. Paper presented at the Proceedings of the 14th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2010).
- Cortina, J. M. (1993). **What is coefficient alpha? An examination of theory and applications**. *Journal of applied psychology*, 78(1), 98.
- D'Arcy, J., & Herath, T. (2011). **A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings**. *European Journal of Information Systems*, 20(6), 643-658.
- Da Veiga, A., & Eloff, J. H. (2010). **A framework and assessment instrument for information security culture**. *Computers & Security*, 29(2), 196-207.
- Davenport, T. H. (2013). **Process innovation: reengineering work through information technology**: Harvard Business Press.
- Dayarathna, R. (2009). **The principle of security safeguards: Unauthorized activities**. *Computer Law & Security Review*, 25(2), 165-172.
- de Leeuw, K. M. M., & Bergstra, J. (2007). *The history of information security: a comprehensive handbook*: Elsevier.

- Dey, M. (2007). *Information security management-a practical approach*. Paper presented at the AFRICON 2007.
- Dhillon, G., & Backhouse, J. (2001). **Current directions in IS security research: towards socio-organizational perspectives**. *Information Systems Journal*, 11(2), 127-153.
- dos Santos Moreira, E., Martimiano, L. A. F., dos Santos Brandão, A. J., & Bernardes, M. C. (2008). **Ontologies for information security management and governance**. *Information Management & Computer Security*, 16(2), 150-165.
- Duggan, G. B., Johnson, H., & Grawemeyer, B. (2012). **Rational security: Modelling everyday password use**. *International Journal of Human-Computer Studies*, 70(6), 415-431.
- Duggan, G. B., Johnson, H., & Sørli, P. (2013). **Interleaving tasks to improve performance: Users maximise the marginal rate of return**. *International Journal of Human-Computer Studies*, 71(5), 533-550.
- Dunphy, P. (2013). *Usable, Secure and Deployable Graphical Passwords* (Vol. 1): Newcastle University PhD Thesis.
- Eastman, C., Teicholz, P., Sacks, R., & Liston, K. (2011). *BIM handbook: A guide to building information modeling for owners, managers, designers, engineers and contractors*: Wiley. com.

- Ensor, B., Montez, T., & Wannemacher, P. (2012). **The state of mobile banking 2012.** *Forrester research. Cambridge, USA.*
- Epstein, M. J. (2008). *Making sustainability work: Best practices in managing and measuring corporate social, environmental, and economic impacts:* Berrett-Koehler Store.
- ERIC, M., & Goetz, E. (2007). **Embedding information security into the organization.**
- Ericsson, G. N. (2007). **Toward a framework for managing information security for an electric power utility—CIGRÉ experiences.** *Power Delivery, IEEE Transactions on*, 22(3), 1461-1469.
- Farroha, B. S., & Farroha, D. L. (2010). *Cyber security framework for enterprise system development: Enhancing domain security through ESM.* Paper presented at the MILITARY COMMUNICATIONS CONFERENCE, 2010-MILCOM 2010.
- Farroha, B. S., & Farroha, D. L. (2010). *Enterprise systems security management: a framework for breakthrough protection.* Paper presented at the SPIE Defense, Security, and Sensing.
- Feng, N., Wang, H. J., & Li, M. (2014). **A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis.** *Information Sciences*, 256, 57-73.

- Fenton, J., & Wolfe, J. (2007). **Organizing for success: some human resources issues in information security.** *Information security management handbook*, 6, 1327-1338.
- Fisher, C., Lauría, E., & Chengalur-Smith, S. (2012). *Introduction to information quality*: Authorhouse.
- Flowerday, S., & von Solms, R. (2005). **Real-time information integrity=system integrity+data integrity+continuous assurances.** *Computers & Security*, 24(8), 604-613. doi: 10.1016/j.cose.2005.08.004
- Flynn, L., Porter, G., & DiFatta, C. (2014). **Cloud Service Provider Methods for Managing Insider Threats: Analysis Phase II, Expanded Analysis and Recommendations.**
- Fourie, L. (2003). **The Management of Information Security—A South African Case Study.** *South African Journal of Business Management*, 34(2), 19.
- Furnell, S. (2008). *Securing information and communications systems: Principles, technologies, and applications*: Artech House.
- Gelbstein, D. E. (2013). *Information security for non-technical managers* R. J. Harrod & S. Baldi (Eds.), (pp. 75).
- Gillies, A. (2011). **Improving the quality of information security management systems with ISO27000.** *The TQM Journal*, 23(4), 367-376.

- Gliem, J. A., & Gliem, R. R. (2003). *Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales.*
- Goel, S., & Chengalur-Smith, I. N. (2010). **Metrics for characterizing the form of security policies.** *The Journal of Strategic Information Systems, 19(4)*, 281-295.
- Golafshani, N. (2003). **Understanding reliability and validity in qualitative research.** *The qualitative report, 8(4)*, 597-607.
- Greitzer, F. L., & Hohimer, R. E. (2011). **Modeling Human Behavior to Anticipate Insider Attacks.** *Journal of Strategic Security, 4(2)*.
- Guardian, T. (1989). **Ronald Reagan.** 2013, from http://en.wikiquote.org/wiki/Ronald_Reagan
- Gupta, A., & Hammond, R. (2005). **Information systems security issues and decisions for small businesses: an empirical examination.** *Information Management & Computer Security, 13(4)*, 297-310.
- Harkins, M. (2012). *Managing Risk and Information Security: Protect to Enable:* Apress.
- Herath, T., Herath, H., & Bremser, W. G. (2010). **Balanced scorecard implementation of security strategies: a framework for IT security performance management.** *Information Systems Management, 27(1)*, 72-81.

- Herath, T., & Raghav Rao, H. (2010). **Control mechanisms in information security: a principal agent perspective.** *International Journal of Business Governance and Ethics*, 5(1), 2-13.
- Herath, T., & Rao, H. R. (2009). **Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness.** *Decision Support Systems*, 47(2), 154-165.
- Hoo, K. J. S. (2000). *How much is enough? A risk management approach to computer security*: Stanford University.
- Ifinedo, P. (2012). **Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory.** *Computers & Security*, 31(1), 83-95.
- IISIT, I. S. a. I. T. (2008). *Setting Knowledge Free Vol. 5*. E. Cohen (Ed.) *The Journal of Issues in Informing Science and Information Technology*
- ISO®. (2013). **ISO 27001 Certification.** 2013, from <http://www.iso27001certificates.com>
- ISO®. (2013). **information technology -- Security techniques -- Code of practice for information security controls.** 2013, from http://www.iso.org/iso/catalogue_detail?csnumber=54533
- It, B. t. C. I. f., BCS, & IT, T. C. I. f. (2011). *Mobile Computing: Securing Your Workforce*: BCS, The Chartered Institute.

- Jamieson, S. (2004). **Likert scales: how to (ab) use them.** *Medical education*, 38(12), 1217-1218.
- Jansen, W., & Grance, T. (2011). **Guidelines on security and privacy in public cloud computing.** *NIST Special Publication*, 800, 144.
- Järveläinen, J. (2012). **Information security and business continuity management in interorganizational IT relationships.** *Information Management & Computer Security*, 20(5), 332-349.
- Järveläinen, J. (2013). **IT incidents and business impacts: Validating a framework for continuity management in information systems.** *International Journal of Information Management*, 33(3), 583-590.
- Johnston, A. C., & Hale, R. (2009). **Improved security through information security governance.** *Communications of the ACM*, 52(1), 126-129.
- Jones, & Learning, B. (2011). *Fundamentals of Information Systems Security*: Jones & Bartlett Publishers.
- Jones, A. (2006). **The Information Security Forum.** *Infosecurity Today*, 3(6), 38-40.
- Kankanhalli, A., Teo, H.-H., Tan, B. C., & Wei, K.-K. (2003). **An integrative study of information systems security effectiveness.** *International Journal of Information Management*, 23(2), 139-154.

- Khan, Q. R. (2012). **Analyzing and Interpreting the Threat Mitigation Strategies in Information Systems Conceptual and Operational Explorations.**
- Kiefer, K. (2004). *Information security: a legal, business, and technical handbook.*
- Kleidermacher, D., & Kleidermacher, M. (2012). *Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development:* Elsevier.
- Kotter, J. P. (2008). *Corporate culture and performance:* SimonandSchuster.com.
- Kruger, H., & Kearney, W. (2006). **A prototype for assessing information security awareness.** *Computers & Security*, 25(4), 289-296.
- Lawton, G. (2008). **New technology prevents data leakage.** *Computer*, 41(9), 14-17.
- Lean-Ping, O., & Chien-Fatt, C. (2014). Information Security Awareness: An Application of Psychological Factors—A Study in Malaysia.
- Leimeister, S. (2010). *IT outsourcing governance: Client types and their management strategies:* Springer.
- Li, H., Zhang, J., & Sarathy, R. (2010). **Understanding compliance with internet use policy from the perspective of rational choice theory.** *Decision Support Systems*, 48(4), 635-645.

- Likert, R. (1974). **A method of constructing an attitude scale.** *Scaling: A sourcebook for behavioral scientists*, 21-43.
- Line, M. B., Tondel, I. A., & Jaatun, M. G. (2011). **Cyber security challenges in Smart Grids.** Paper presented at the Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on.
- MacKinnon, L., Bacon, L., Gan, D., Loukas, G., Chadwick, D., & Frangiskatos, D. (2013). **Cyber security countermeasures to combat cyber terrorism.** *Akhgar B and Yates S. Strategic Intelligence Management. Butterworth-Heinemann, London*, 234-257.
- Maizlish, B., & Handler, R. (2010). **IT (Information Technology) Portfolio Management Step-by-Step: Unlocking the Business Value of Technology:** John Wiley & Sons.
- Mather, T., Kumaraswamy, S., & Latif, S. (2009). **Cloud security and privacy: an enterprise perspective on risks and compliance:** " O'Reilly Media, Inc."
- Mayer, N., Heymans, P., & Matulevicius, R. (2007). **Design of a Modelling Language for Information System Security Risk Management.** Paper presented at the RCIS.
- McIlwraith, A. (2006). Information security and employee behaviour. **How to reduce risk through employee education, training and awareness.**

- Mirkovic, J., Dietrich, S., Dittrich, D., & Reiher, P. (2004). *Internet Denial of Service: Attack and Defense Mechanisms (Radia Perlman Computer Networking and Security)*: Prentice Hall PTR.
- Mishra, S., & Dhillon, G. (2006). *Information systems security governance research: a behavioral perspective*. Paper presented at the 1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference.
- Muller, I., Han, J., Schneider, J.-G., & Versteeg, S. (2011). *Tackling the Loss of Control: Standards-Based Conjoint Management of Security Requirements for Cloud Services*. Paper presented at the Cloud Computing (CLOUD), 2011 IEEE International Conference on.
- Oberheide, J., Veeraraghavan, K., Cooke, E., Flinn, J., & Jahanian, F. (2008). *Virtualized in-cloud security services for mobile devices*. Paper presented at the Proceedings of the First Workshop on Virtualization in Mobile Computing.
- Ozkan, S., & Karabacak, B. (2010). **Collaborative risk method for information security management practices: A case context within Turkey**. *International Journal of Information Management*, 30(6), 567-572.
- Parmenter, D. (2010). *Key performance indicators (KPI): developing, implementing, and using winning KPIs*: John Wiley & Sons.

- PCI, S. S. C. (2013). **PCI DSS Data Security Standards Overview**.
from https://www.pcisecuritystandards.org/security_standards/index.php
- Peltier, T. R. (2013). *Information security fundamentals*: CRC Press.
- Peltier, T. R. (2013). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*: CRC Press.
- Pfleeger, C. P., & Pfleeger, S. L. (2006). *Security in computing*: Prentice Hall PTR.
- Pfleeger, C. P., & Pfleeger, S. L. (2012). *Analyzing Computer Security: A Threat-Vulnerability-Countermeasure Approach*: Prentice Hall Professional.
- PMA, P. M. A. (2013). **Banks' Directory**. 2013, from <http://www.pma.ps/ar-eg/banksdirectory.aspx>
- Poolsappasit, N., Dewri, R., & Ray, I. (2012). **Dynamic security risk management using bayesian attack graphs**. *Dependable and Secure Computing, IEEE Transactions on*, 9(1), 61-74.
- Post, G. V., & Kagan, A. (2007). **Evaluating information security tradeoffs: Restricting access can interfere with user tasks**. *Computers & Security*, 26(3), 229-237.

- Posthumus, S., & Von Solms, R. (2004). **A framework for the governance of information security.** *Computers & Security*, 23(8), 638-646.
- Qian, Y., Fang, Y., & Gonzalez, J. J. (2012). **Managing information security risks during new technology adoption.** *Computers & Security*, 31(8), 859-869.
- Radovanovic, D., Radojevic, T., Lucic, D., & Sarac, M. (2010). **IT audit in accordance with Cobit standard.** Paper presented at the MIPRO, 2010 Proceedings of the 33rd International Convention.
- Randone, E. (2011). **The Effect of Internal Training from the Employee's Point of View.**
- Rashidi, P., Cook, D. J., Holder, L. B., & Schmitter-Edgecombe, M. (2011). **Discovering activities to recognize and track in a smart environment.** *Knowledge and Data Engineering, IEEE Transactions on*, 23(4), 527-539.
- Rastogi, R., & Von Solms, R. (2012). **Information Security Service Management.** *Journal of Contemporary Management*, 9, 257-278.
- Ratner, B. D., Cohen, P., Barman, B., Mam, K., Nagoli, J., & Allison, E. H. (2013). **Governance of Aquatic Agricultural Systems: Analyzing Representation, Power, and Accountability.** *Ecology and Society*, 18(4), 59.

- Ren, P., & Du, Z. (2013). ***Information Technology and Industrial Engineering (Set)*** (Vol. 48): WIT Press.
- Rezakhani, A., Hajebi, A., & Mohammadi, N. (2011). **Standardization of all Information Security Management Systems**. *International Journal of Computer Applications*, 18(8).
- Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). **Unrealistic optimism on information security management**. *Computers & Security*, 31(2), 221-232.
- Risvold, M. O. (2010). **Organizational issues related to information security behavior**. *Lulea University of Technology*.
- Rodriguez, C., & Martinez, R. (2013). **The Growing Hacking Threat to Websites: An Ongoing Commitment to Web Application Security**. *Frost & Sullivan*. Retrieved, 13.
- Roos, C. J. (2013). **Governance responses to hacking in the banking sector of South Africa: an exploratory study**.
- Sánchez, L. E., Parra, A. S.-O., Rosado, D. G., & Piattini, M. (2009). Managing Security and its Maturity in Small and Medium-sized Enterprises. *J. UCS*, 15(15), 3038-3058.
- Sasse, M. A., Brostoff, S., & Weirich, D. (2001). **Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security**. *BT technology journal*, 19(3), 122-131.

- Sawalha, I. H. (2011). *Business Continuity Management and Strategic Planning: the Case of Jordan*. University of Huddersfield.
- Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., & Sommerlad, P. (2013). *Security Patterns: Integrating security and systems engineering*: John Wiley & Sons.
- Seker, H. (2012). *Engineering approach to risk management in information technology systems*.
- Senft, S., & Gallegos, F. (2010). *Information technology control and audit*: CRC Press.
- Shabtai, A., Elovici, Y., & Rokach, L. (2012). **Data Leakage Detection/Prevention Solutions A Survey of Data Leakage Detection and Prevention Solutions** (pp. 17-37): Springer.
- Sharma, S. K., & Sefchek, J. (2007). **Teaching information systems security courses: A hands-on approach**. *Computers & Security*, 26(4), 290-299. doi: <http://dx.doi.org/10.1016/j.cose.2006.11.005>
- Shirtz, D., & Elovici, Y. (2011). **Optimizing investment decisions in selecting information security remedies**. *Information Management & Computer Security*, 19(2), 95-112.
- Silic, M., & Back, A. (2013). **Factors impacting information governance in the mobile device dual-use context**. *Records Management Journal*, 23(2), 73-89.

- Sinclair, S., Smith, S. W., Trudeau, S., Johnson, M. E., & Portera, A. (2008). **Information risk in financial institutions:** Field study and research roadmap *Enterprise Applications and Services in the Finance Industry* (pp. 165-180): Springer.
- Singh, A. (2012). **Trust Management and Security Access Controls in High Payload System Architecture.** *International Journal of Engineering Research and Applications (IJERA)*.
- Sipior, J. C., & Ward, B. T. (2008). **A Framework for Information Security Management Based on Guiding Standards: A United States Perspective.** *Issues in Informing Science and Information Technology*, 5, 51-60.
- Siponen, M., Adam Mahmood, M., & Pahlila, S. (2014). **Employees' adherence to information security policies: An exploratory field study.** *Information & Management*, 51(2), 217-224.
- Siponen, M., & Willison, R. (2009). **Information security management standards: Problems and solutions.** *Information & Management*, 46(5), 267-270.
- Siponen, M. T. (2005). **Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods.** *Information and organization*, 15(4), 339-375.

- Spremić, M. (2009). **IT governance mechanisms in managing IT business value.** *WSEAS Transactions on Information Science and Applications*, 6(6), 906-915.
- Stamp, M. (2011). *Information security: principles and practice*: John Wiley & Sons.
- Stellar, J. E., Manzo, V. M., Kraus, M. W., & Keltner, D. (2012). **Class and compassion: socioeconomic factors predict responses to suffering.** *Emotion*, 12(3), 449.
- Stewart, J. M., Chapple, M., & Gibson, D. (2012). *CISSP: Certified Information Systems Security Professional Study Guide*: John Wiley & Sons.
- Stouffer, K., Falco, J., & Scarfone, K. (2011). **Guide to industrial control systems (ICS) security.** *NIST Special Publication*, 800-882.
- Sui, Y., Zou, X., Du, Y., & Li, F. (2012). **Design and analysis of a highly user-friendly, secure, privacy-preserving, and revocable authentication method.** *IEEE Transactions on Computers* (submitted, 2012).
- Systems, C. R. (1982). **Sample Size Calculator.** 2013, from <http://www.surveysystem.com/sscalc.htm>
- Tayeh, A. M. (2008). **Effectiveness of Information Security Management at the Palestinian Information Technology Companies.**

- Teece, D. J. (2010). **Business models, business strategy and innovation.** *Long range planning*, 43(2), 172-194.
- Thomson, K.-L., & Von Solms, R. (2003). **Integrating information security into corporate culture.** *Unpublished. Masters dissertation, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa.*
- Thomson, K.-L., & von Solms, R. (2005). **Information security obedience: a definition.** *Computers & Security*, 24(1), 69-75. doi: 10.1016/j.cose.2004.10.005
- Tipwong, P. (2011). **Reducing Data Loss and Saving Money by Acquiring Data Loss Prevention Software.**
- Topi, H., Valacich, J. S., Wright, R. T., Kaiser, K., Nunamaker Jr, J. F., Sipior, J. C., & de Vreede, G.-J. (2010). **Communications of the Association for Information Systems.**
- Van Niekerk, J. F. (2011). *Fostering information security culture through intergrating theory and technology.*
- Van Niekerk, J. F., & Von Solms, R. (2010). **Information security culture: A management perspective.** *Computers & Security*, 29(4), 476-486. doi: 10.1016/j.cose.2009.10.005
- von Solms, B., & von Solms, R. (2004). **The 10 deadly sins of information security management.** *Computers & Security*, 23(5), 371-376. doi: 10.1016/j.cose.2004.05.002

- Von Solms, B., & von Solms, R. (2005). **From information security to... business security?** *Computers & Security*, 24(4), 271-273.
- von Solms, B., & von Solms, R. (2005). **From information security to...business security?** *Computers & Security*, 24(4), 271-273. doi: 10.1016/j.cose.2005.04.004
- Von Solms, R. (1999). **Information security management: why standards are important.** *Information Management & Computer Security*, 7(1), 50-58.
- von Solms, R., & von Solms, S. H. (2006). **Information Security Governance: A model based on the Direct–Control Cycle.** *Computers & Security*, 25(6), 408-412.
- von Solms, R., & von Solms, S. H. (2006). **Information security governance: Due care.** *Computers & Security*, 25(7), 494-497.
- Weinman, J. (2012). *Clouconomics: The Business Value of Cloud Computing*: John Wiley & Sons.
- Werlinger, R., Hawkey, K., & Beznosov, K. (2009). **An integrated view of human, organizational, and technological challenges of IT security management.** *Information Management & Computer Security*, 17(1), 4-19.
- Whitman, M., & Mattord, H. (2013). *Management of information security*: Cengage Learning.

- Whitman, M. E., & Mattord, H. J. (2010). *Management of information security*: CengageBrain. com.
- Yazdanifard, R., Musa, M. G., & Molamu, T. (2011). *The Basics Issues on the Security Information Management Practices in Organizational Environment*. Paper presented at the Management and Service Science (MASS), 2011 International Conference on.
- Yeniman Yildirim, E., Akalp, G., Aytac, S., & Bayram, N. (2011). **Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey**. *International Journal of Information Management*, 31(4), 360-365.
- YOYO. (2010). **The CIA triangle**. 2014, from http://www.talktoanit.com/c_old/index.php?option=com_content&view=article&id=145:el-triangulo-de-cia&catid=44:cosa-de-dia-a-dia&Itemid=83
- Zissis, D., & Lekkas, D. (2012). **Addressing cloud computing security issues**. *Future Generation Computer Systems*, 28(3), 583-592.
- بحيصي، ع.، & شعبان، ح. (2008). *مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المصارف العاملة في قطاع غزة*. مجلة الجامعة الإسلامية (سلسلة الدراسات الإنسانية)، المجلد السادس عشر (العدد الثاني)، ص 895 - ص 923 .
- مصلح، ر. م. خ. (2013). *مدى توافر متطلبات أمن البيانات و المعلومات المحاسبية و وسائط تخزينها الآلية في البنوك الأردنية: دراسة ميدانية* .

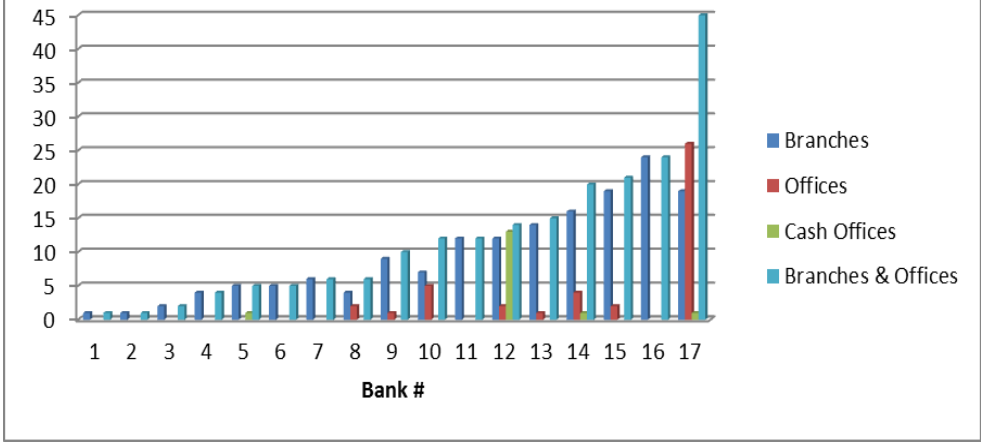
Appendices

Appendix A:

Overview about branches and offices for Palestinian banks (PMA, 2013)

Bank #	Bank Name
1	HSBC Bank Middle East Limited
2	Union Bank
3	Jordan Kuwait Bank
4	Jordan Commercial Bank
5	The National Bank
6	Jordan Ahli Bank
7	Palestine Commercial Bank
8	Egyptian Arab Land Bank
9	Arab Islamic Bank
10	Palestine Investment Bank
11	The Housing Bank for Trade & Finance
12	Bank of Jordan
13	Palestine Islamic Bank
14	Al-Quds Bank
15	Cairo Amman Bank
16	Arab Bank
17	Bank of Palestine P.L.C

Palestinian banks



Appendix B:
Questionnaire of
Status and Effectiveness of Information Security Management
In Palestinian Banks

Dear Sir/Mrs.

The researcher is doing a study on the status of information security management in Palestinian banks, as well as the factors that influence the effectiveness of information security management process.

In order to achieve that, the researcher designed this questionnaire, which is segmented in to three parts; the first one is general information, the second part aimed to test the current state of Information Security Management in the Palestinian banks, where the third part aims to measure the achieving of effective Information Security Management through five domains (People, Process, Products/Technology, Partners/Suppliers, and Data).

The questionnaire is intended to measure administrative issues, so it's oriented to whom working in administrative, risk, compliance, information security, and information technology jobs.

I would appreciate your answers to this questionnaire and stress that you will be making a great service to the research process in the Palestinian universities.

We believe that you are the best source to reach the required information, which serves our community and its development. We all hope to find cooperation from you through answering the questions contained in this survey. We pledge not to enclose the identity of participants to third party, as well as not use this information in any field except scientific research.

Best Regards,

Researcher

Information Security Management

Please put x letter in the box that related to your answer.

First: General Information

I. Personal Information

1. Qualification:

Diploma or less

Bachelor

High Education

2. Specialty:

Administration

Engineering

IT

other (please

specify).....

3. Experience years:

5 years or less

6 - 10 years

11 - 15 years

More than 15

years

4. Carrying certifications related to information security: Yes No

(Incase **yes** please list specify.....)

5. Work Field.

Administrative

Technical

II. Organizational Information

6. Number of the bank Branches/Offices.

5 branches or less 6 - 10 branches 10 to 19 branches 20 or more

branches

7. The Bank holding International Information Security Management

standard: Yes No

Incase yes please choose:

ISO PCI COBIT ITIL other

specify.....

Second: Current State of Information Security Management.

To what extent do these controls applied to achieve Information Security Management?

No.	Control	Application degree				
		Very High	High	Moderate	Low	Very Low
8.	Definition of information security roles & responsibilities.					
9.	The development of information security policies and procedures within the organization.					
10.	An information and Asset Classification schema such as (Confidential, Private, Personal Public).					
11.	Users training & awareness e.g. Internet threats, spear phishing socially engineered email					
12.	Management and inventory of authorized and unauthorized devices, systems, software, etc.					
13.	Patching, updating and upgrading of applications, device OSs, and operating systems.					
14.	Secure configurations on computers. Such as antivirus, encryptions, firewalls.					
15.	The use of host based controls to improve the security and auditing on endpoints. Such as Intrusion Detection/Prevention System, firewall. etc.					
16.	Network devices secure configuration. Such as VLANS, Encryption, Tunnels, password encryption					

No.	Control	Application degree				
		Very High	High	Moderate	Low	Very Low
17.	Vulnerability assessment and management.					
18.	The use of perimeter, system, endpoint and mobile devices malware inspection and protection.					
19.	Encryption of confidential data and information.					
20.	Application control by whitelisting of application e.g. by using Microsoft Software Restriction Policies.					
21.	The implementation of a backup and recovery plan within the organization.					
22.	Secure network design using concepts such as segregation, zoning, filtering, monitoring.					
23.	The control of wireless access within the organization.					
24.	Monitoring and analysis of security audit logs.					
25.	Controlled administrative privileges for the IT team on the servers and data.					
26.	Data integrity checking.					
27.	Data loss prevention plan.					
28.	Having an internal and external penetration testing exercise.					
29.	Email usage control with email malware and Anti-Spam detection and quarantine.					
30.	Web content filtering of incoming and outgoing traffic.					
31.	User access control and privileges.					
32.	Encryption for server-to-server and client-to-server communication.					

Third: Effectiveness of Information Security Management

To what extent do you think these factors influence the Effectiveness of Information Security Management?

No.	Factor	Effectiveness degree				
		Very High	High	Mode rate	Low	Very Low
Domain One: People						
33.	Security and academic checks at the time of recruitment.					
34.	Awareness of information security training courses.					
35.	Logical access control procedure and policy.					
36.	Information security policy is approved and known by employees.					
37.	Segregation of duties.					
Domain Two: Processes						
38.	Documentation of information security policy.					
39.	Change management i.e., any change to be made goes through the change control authorization process.					
40.	Documentation of operating procedures.					
41.	Including information security in the business continuity management process.					
42.	Risk assessment and management.					
Domain Three: Products/Technology						
43.	Physical and environmental security management.					
44.	Equipment security management.					
45.	Access controls management.					
46.	Protection against malicious software.					
47.	Backup and recovery management.					
Domain Four: Partners/Suppliers						
48.	Addressing security when dealing with customers.					

No.	Factor	Effectiveness degree				
		Very High	High	Moderate	Low	Very Low
49.	Third party service delivery management.					
50.	System acceptance such as new information systems, upgrades and new versions.					
51.	Supplier profile and qualification check in addition to service registration and staff qualification certificates.					
52.	Define Service level agreement with all suppliers and 3 rd parties.					
Domain Five: Data						
53.	Secure data at rest and in motion.					
54.	Data masking in test and developments environment.					
55.	Apply very strong policy and procedures for IT staff specially the DBA when accessing the data.					
56.	Sign NDA with the vendors especially when they need to access the data.					
57.	Data labeling and handling in accordance with the classification scheme adopted by the organization.					

Thank you very much for your time

Appendix C: Arbitrators and experts who reviewed the questionnaire

Name	Position	Organization Name
Dr. Baker Abdalhaq	Dean of faculty of Information Technology	An Najah National University
Dr. Husam Arman	Associate Research Specialist	Kuwait Institute for Scientific Research
Dr. Ma'zoz Alawneh	Associated Professor / Measurement and Evaluation	Al-Quds Open University
Eng. Fares Hindi	IT department deputy director	Palestine Monetary Authority
Eng. Mustafa A. Khaizaran	Manager of Network and Systems Department	Arab Islamic Bank
Eng. Nael Hamaydeh	Senior System Engineer	The Housing Bank for Trade & Finance

Appendix D: Information Security Standards and Best Practices

According to Dey (2007), a list of some of them with a brief definition:

- ✓ Sarbanes-Oxley Act (SOX) – compulsorily applies to all public companies
- ✓ Health Insurance Portability and Accountability Act (HIPAA) – applies to any organization handling health information about an individual
- ✓ Gramm-Leach-Bliley Act (GLBA) – applies to any financial institution and the companies that provide services to the institution
- ✓ California Security Breach Notice Act (formerly SB 1386) – requires companies maintaining data on California residents to inform individuals of any security breaches associated with their personal information
- ✓ European Safe Harbor Registration (European Data Protection) – data safety norms for all international firms with offices both in the US and in the EU
- ✓ Homeland Security Presidential Directives (HSPD- 12) – directives for a common identification standard for US Federal employees and contractors
- ✓ Federal Financial Institution Examination Council (FFIEC) – guidelines for enhanced multilayer authentication procedure for banking institution

- ✓ The Committee of Sponsoring Organization of the Tradeway Commission (COSO) – common definition of internal control, standards and criteria against which organizations can assess their control systems
- ✓ Payment Card Industry (PCI), Data Security Standards (DSS) - govern the security standards for the most payment industries (Visa, MasterCard, etc.)
- ✓ Freedom of Information Acts 2000 - UK government legislation defining what information public sector organizations are obliged to provide on request
- ✓ Federal Information Security management Act (FISMA) – US Federal law as e-government Act, imposes a mandatory set of processes to be followed
- ✓ Control Objectives for Information and Related Technology (COBIT) – best practices for better control, audit and measurement
- ✓ The Information Technology Infrastructure Library (ITIL) – best practices for better IT services
- ✓ Information Security Forum's (ISF) Standard of Good Practice – guide to manage the business risks associated with organization's information systems

- ✓ Statement of Auditing Standards (SAS) 70 – defines the audit standards in order to assess the contracted internal controls of a service organization.

جامعة النجاح الوطنية

كلية الدراسات العليا

إدارة أمن المعلومات في البنوك الفلسطينية

إعداد

عبداللطيف لطفي محسن

إشراف

د. فادي دريدي

قدمت هذه الأطروحة استكمالاً لمتطلبات الحصول على درجة الماجستير في الإدارة الهندسية
بكلية الدراسات العليا في جامعة النجاح الوطنية في نابلس، فلسطين.

2014

ب

إدارة أمن المعلومات في البنوك الفلسطينية

إعداد

عبداللطيف لطفي محسن

إشراف

د. فادي دريدي

الملخص

تزايد في الآونة الأخيرة اعتماد المؤسسات على التكنولوجيا والاتصالات والمعلومات، ترافق ذلك مع ازدياد الاختراقات والتهديدات والهندسة الاجتماعية؛ لذلك أصبح أمن المعلومات من القضايا التي تحتل المراتب الأولى في خطط إدارة المؤسسات، بل وفي التخطيط الاستراتيجي لها، ولما كانت البنوك من أهم القطاعات التي تعتمد على المعلومات، ومن أهم القطاعات في فلسطين، تم اختيار إدارة أمن المعلومات في البنوك الفلسطينية لتكون مجال هذه الدراسة.

هدفت هذه الدراسة إلى دراسة الوضع الحالي لإدارة أمن المعلومات المتبعة في البنوك الفلسطينية واستعراضها، وقياس درجة تطبيق ضوابط إدارة أمن المعلومات في هذا القطاع، بالإضافة إلى تسليط الضوء على المواضيع المتعلقة بإدارة أمن المعلومات مثل الحوكمة والامتثال والمخاطر، كما هدفت إلى استطلاع آراء المستجيبين حول درجة تأثير مجالات البحث الخمس (الموظفين والإجراءات والتكنولوجيا و"المزودين والشركاء" والبيانات) على فعالية إدارة أمن المعلومات.

استخدم الباحث منهجية التحليل الوصفي؛ لذلك قام بتصميم استبانة لهذا الغرض وتم توزيعها على موظفي دوائر تكنولوجيا المعلومات والتدقيق الداخلي في الإدارات العامة للبنوك العاملة في فلسطين، المرخصة من سلطة النقد الفلسطينية، حيث تم توزيع 94 استبانة استرجع منها 82 استبانة صالحة للتحليل، بمعدل استجابة 87%.

وقد أظهرت النتائج أن البنوك الفلسطينية تقوم بتطبيق ضوابط إدارة أمن المعلومات بدرجة عالية، إلا أن ضابط "التدريب والتوعية للموظفين"، وضابط "فحص تكامل البيانات" كان تطبيقهما بدرجة متوسطة، كما توصلت الدراسة إلى أن البنوك التي لديها (10-19) فرعاً هي أكثر البنوك الفلسطينية تطبيقاً لضوابط إدارة أمن المعلومات، كما توصلت إلى أن البنوك التي تتبع معيار إدارة أمن معلومات عالمي أكثر تطبيقاً لضوابط إدارة أمن المعلومات من غيرها.

كما توصلت الدراسة إلى أن مجال العنصر البشري هو أكثر المجالات تأثيراً على فعالية إدارة أمن المعلومات، ويربط هذه النتيجة مع كون ضابط "التدريب والتوعية للموظفين" يطبق بدرجة متوسطة، فإن هذا يقود إلى حاجة البنوك الفلسطينية إلى مزيد من الدورات التدريبية و التوعوية الخاصة بأمن المعلومات للموظفين.

كما خلصت الدراسة إلى توصية البنوك الفلسطينية إعطاء ضابط "فحص تكامل البيانات" أهمية أعلى، كما توصي الدراسة البنوك الفلسطينية باتباع معايير إدارة امن المعلومات العالمية لما لها من تأثير في الالتزام في تطبيق ضوابط إدارة أمن المعلومات.