

The Impact of Implementing Information Security Management Systems on E-Business Firms: Case Study in Jordanian banking sector.

أثر تطبيق أنظمة إدارة أمن المعلومات على الأعمال الإلكترونية للشركات: دراسة حالة في قطاع البنوك الأردنية.

Prepared by

Suhail H. Alabed

Supervisor

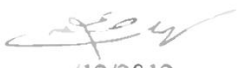
Dr. Raed Hanandeh

THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
Master on E-Business.

December 2013

Authorization

I am Suhail H. Alabed; authorize Middle East University to make copies of my dissertation to libraries, institutions, or public when asked to.

Name	Suhail H Alabed
Signature	
Date	/12/2012

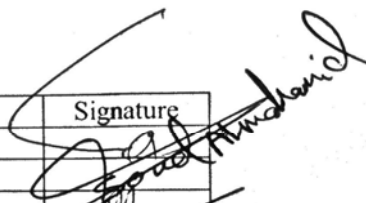


DISCUSSION COMMITTEE DECISION

This thesis was discussed under title:

The Impact of Implementing Information Security Management Systems on E-Business Firms: Case Study in Jordanian banking sector.

Approved on

Date: 10/3/2013

Discussion Committee		University	Signature
Dr. Raed Hanandeh	Supervisor	MEU	
Dr. Soud Almahamid	Internal Member	MEU	
Dr. Haroun Alryalat	External Member	The World Islamic Science & Education University.	

Acknowledgements

This thesis is the product of an educational experience at MEU, various individuals have contributed towards its completion at different stages, either directly or indirectly,. Any attempt to thank all of them is bound to fall short.

To begin, I would like to express my wholehearted and sincere gratitude to Dr. Raed Hanandeh for his guidance, time and patience, for supporting participants in this thesis during all stages of performance.

I would like to extend my special thanks to my tutor, whose encouragement and support were vital, without which I wouldn't be able to completing this degree's requirements to bring it in its current mode.

Sincerely Yours:

Suhail H. Alabed.

Dedication

To

My Father and Mother

My Wife, Son, and Daughters

All my Family Members

And To my best Friend Ismail Mohammed.

Sincerely Yours,

Suhail H. Alabed

Table of Contents

Table of Contents

Authorization	I
DISCUSSION COMMITTEE DECISION.....	II
Acknowledgements.....	III
Dedication	IV
Table of Contents.....	V
List of t Tables	VII
List of Figures	VIII
Appendices.....	IX
Abstract.....	X
General Framework.....	1
1.1: Introduction.....	2
1.3: Study Significance.....	5
1.4: Study Objectives.....	6
1.5 Study Model and Hypothesis.....	8
1.6: Study Limitations.....	10
1.7: Study Delimitations (Difficulties).....	10
1.8: Terminologies.....	11
Chapter Two.....	13
Theoretical Framework and Previous Studies.....	13
2.1: Introduction.....	14
2.2 Information:	15
2.3 Information Security System.....	20
2.6 literature review	44
2.7 Study Contribution to knowledge.....	52
Chapter Three.....	53
Method and Procedures.....	53
3-1: Introduction.....	54
3-2: Study Methodology.....	54

3-4: Study Tools and Data Collection.....	55
3-5: Statistics treatment.....	58
3-6: Validity and Reliability.....	59
Chapter Four.....	61
Analysis Result and Hypotheses Test.....	61
4-1: Introduction.....	62
4-2. Study Questions answers:.....	62
4-4: Study Hypotheses Test.....	70
Chapter Five.....	76
Results and Recommendations.....	76
Chapter Five.....	77
5-1: Results.....	77
Appendices.....	86
Appendix 1.....	86
Appendix 2.....	91
Appendix 3.....	92

List of t Tables

No.	Subject	Page
2-1	Major Information Security Incidents.	17
3-1	Reliability of Questionnaire Dimensions	57
4-1	Distribution of research sample according to demographic variables.	61
4-2	Samples' Distributions in terms of Security Policy	62
4-3	Descriptive Statistic of Internal Audit as to the Research Sample.	63
4-4	Descriptive Statistic of External Audit as to the Research Sample.	64
4-5	Internal Attack Vulnerability	65
4-6	External Attack Vulnerability for the Research Companies.	66
4-7	Intrusions detection success	67
4-8	Viewing the System is Secure	67
4-9	Simple Regression between information security management system and E-Business security firms.	68
4-10	Stepwise Multiple Regression test to identify the effect of security management system on vulnerability of internal attack	69
4-11	Stepwise Multiple Regression test to identify the effect of security management system on vulnerability of external attack.	70
4-12	Stepwise Multiple Regression test to identify the effect of security management system on intrusion detection success.	71
4-13	Stepwise Multiple Regression test to identify the effect of security management system on viewing better secure system.	72

List of Figures

No.	Subject	Page
1-1	Study Model	9
2-1	2011 Sampling of Security Incidents by Attacks Type, Time, and Impact,	19
2-2	Security elements.	21
2-3	Information Security Conceptual Architecture.	23
2-4	PDCA diagram	28
2-5	Risk relationships.	29
2-6	Control Clauses	30
2-7	ISMS implementation process' cycle.	35

Appendices

No.	Subject	Page
1	Information Security Management System (ISMS) family standards, scope and purpose.	92
2	Names of arbitrators.	97
3	Questionnaire.	98

***The Impact of Implementing Information Security
Management's Systems in E-Business Firms.***

Case Study in Jordanian banking sector.

Prepared by

Suhail H. Alabed

Supervisor

Dr. Raed Hanandeh

Abstract

The main objective of this study is to understand the impact of applying Information Security Management Systems on E-business security firms. The targeted employees sector as to this research, is directed towards all IT banking Staff in Jordan. A random sample of the respective employees was selected to consist of (116) IT professionals in Jordanian Commercial banks. In my way to fulfill the research objectives, a Questionnaire was processed to collect relevant data in terms of this research's variables. The outcomes of foregoing questionnaire stated that most of respondents believe that their organization adopts corporate security policy, including but not limited to, regular internal and external audit to maintain the organization systems and protect it against, both internal and external violations. Furthermore, the availability of security systems in any organization shall work in hastening the concerned employees to review their organization systems, supported with to Managers' approval and recommendations to obtain wide range of security.

المخلص باللغة العربية

أثر تطبيق أنظمة إدارة أمن المعلومات على الأعمال الإلكترونية للشركات: دراسة
حالة في قطاع البنوك الأردنية.

إعداد

سهيل حسين العبد

إشراف

الدكتور رائد هنانده

انصبت هذه الدراسة بشكل أساسي، على فهم أثر تطبيق أنظمة إدارة أمن المعلومات على قطاع الأمن الإلكتروني في الشركات. قطاع الموظفين المستهدف في هذا البحث يشمل أولئك الذين يعملون في قطاع المعلومات الإلكترونية في البنوك الأردنية. تم اختيار عينة عشوائية تتألف من ١١٦ محترف في هذا المجال يعملون في البنوك التجارية الأردنية. بسبب التوصل الى تحقيق كافة متطلبات البحث ، تم اصدر استبيان لجميع بيانات ذات علاقة وثيقة في مجال متغيرات هذا البحث. أظهرت نتائج الاستبيان موضوع البحث، أن معظم المتجاوبين مع الاستبيان يعتقدون ان شركتهم أو مؤسستهم المالية معينة بتطبيق سياسة أمن المعلومات شاملا بدون حصر، تدقيق خارجي وداخلي للمحافظة على أنظمة مؤسستهم وحمايتها من الاختراق الخارجي والداخلي. إضافة إلى ذلك، توفر أنظمة الأمن في أي شركة سيعمل بدون شك، في تسريع عملية استعراض أنظمة شركتهم من قبل الموظفين ذوي العلاقة، تقديم الدعم لهم من قبل المدراء وبالتالي توصية المدراء للحصول على مدى واسع في مجال الأمن المعلوماتي.

Chapter One

General Framework

1.1 Introduction.

1.2 Study Problem and Questions.

1.3 Study Significance.

1.4 Study Objectives.

1.5 Study Model and Hypothesis.

1.6 Study Limitations.

1.7 Study delimitations (Difficulties).

1.8 Terminologies.

1.1: Introduction.

Recently, IT development requires, badly, availability of information systems' (IS) in industrial Sectors. Meanwhile, major concerns came out, increasingly, as to apply information security systems, directed to maintain the information processing safe and sound, in terms of breaches and violations. Such breaches and violations do endanger all various business activities, as well. Accordingly, worldwide companies, especially banking Sector, have increased their investment in IT Security. A most recent forecast indicates that the global market for information security shows increasing investment in IT security; in terms of protecting achieved data, customer's information, and thus the whole business interests (International Data Corporation, 2007).

Information management Security policies should ensure that state and federal regulations are being followed. Besides, handling private and personal information requires engagement of various employees from all sections in the organization. In the same time a plan shall be available to set out reporting process to executive security officers in the organization, as to any breach or violation thereof. Such reporting shall be channeled in four directions; initial assessment of privacy, procedures to be adopted, and methods, which are scheduled to track the flow of employees' personal information. Designated employees, who are also, concerned in securing its confidentiality via security available procedures. In the same time, the probable risks, which originate from the non-application of, or failure to protect, such personal information, shall be identified. (Parker, 2003, p. 47).

Business' practice; via web or online, is still in its first beginning. Practicing business, via web as, a business-to-business (B2B) or business-to-consumer (B2C) commercial medium has been widely explored. However, a critical assessment of related E-business challenges and issues has just started to receive attention; one of the factors that contribute in increasing incidents potential as to E-business-related security, is the “trusted” business partnership. Business partners in a B2B partnership chain can have access to highly confidential back-end resources and information. Consequently, the security challenge migrates from securing the network, to protecting the virtual network. The complexities of these B2B partnerships and relationships are often very onerous and risky (Clarke, 2001).

Organizations should consider the impact on reputation and enterprise value resulting from information security failures. Whilst, Executive Management is engaged to consider and respond to, information security issues, policies inside organization, and increasing expectations thereof. The foregoing shall work on making the information security issue an intrinsic part of the enterprise's governance efforts, focusing on and integrate with processes available to govern other critical functions. Efficient security may work in goodwill improvement, establishing others' confidence; with which the business is conducted, and may improve performance through saving time and efforts that may be exploited to recover from such security incidents (ITGI, 2006).

Internal and external security auditing could be performed; either by in-house or external auditors. Threats to computerized information systems changes from time to time. The Technology changes, the skills are in continuous rising as well, organizations are in continuous and daily process of checking up their systems, designing methods of

solving security identified problems. They are in bad need of Internal audit to check up and cure identified problems and provide recommendations. Also Internal audit is also, engaged in discussing the strategic policies in the company with respective systems suppliers. (Wright, 2007).

The banking sector in Jordan is one of the most important financial sectors in the country. Investment in security technology; E-business is generated widely in this financial sector. Considerable range of information and transactions is exchanged internally; among employees and externally; among other banks of concern. On the other hand, such information is communicable with customers as well. Accordingly, the availability of IT department in the financial institutions who are engaged in managing and maintaining the data security becomes vital.

Information and data are the cornerstone of E-business. The promising E-business is faced by security challenges associated with the disintermediation of data access. Challenges include, but not limited to, the expansion of the data users volume through internet, and so on. The foregoing created urgent demand as to data security and main topic to be discussed in detail.

1.2: Study Problem and Questions.

Most accurate and up-to-date business information outside and inside a traditional firm; is considered risky and may cause dramatic loss once practiced within the common use of banking services presented via internet. In the absence of security system, such transactions may generate mistakes which could hardly be solved. The Information Securing business is a burden as to the IT department and other staff of concern.

This research aims to identify the impact carrying out information Security Management Systems process; Policies and Audits, throughout replying the following questions:

1. Is there a positive impact of Information Security management Systems on E-Business security Firms in banking sector in Jordan?
2. Is there a positive impact of information security management systems (corporate security policies, frequent internal systems security audits, frequent external systems security audits) on vulnerable to attacks by internal parties in banking Sector in Jordan?
3. Is there a positive impact of information security management systems (corporate security policies, frequent internal systems security audits, frequent external systems security audits) on vulnerable to attacks by external parties in banking Sector in Jordan?
4. Is there a positive impact of information security management systems (corporate security policies, frequent internal systems security audits, frequent external systems security audits) on detecting intrusions in banking sector in Jordan?
5. Is there a positive impact of information security management systems (corporate security policies, frequent internal systems security audits, frequent external systems security audits) on more secure system in banking sector in Jordan?

1.3: Study Significance.

E-business works on making information available for the access of customers, partners, and employees, in a controlled and secure method. Managing E-business security is a

multifaceted challenge and requires accurate coordination between business policy and practice in one side and relevant technology in the other side (Oracle, 2002)

Normally, any access to sensitive business information shall be directed through concerned employees. Although the latests may not always be reliable, but their access to sensitive data shall be limited to their jobs function. On the other hand, the access shall be governed by physical and procedural controlling regulations. There should be a disciplinary system applies to Employees who disclose sensitive information to T.P. Such system shall indeed, work on restricting the unauthorized access or disclosure of such information.

E-Business works on making business information available for outsiders. At the same time, it works on same, as to users who are in-need of. Such available access may be performed either internally; employees, or externally; customers, suppliers, employees, or partners) each must benefit of such privileges. (Oracle, 2004)

1.4: Study Objectives.

This study aims to introduce an Information Security Systems model that will help banking sector in Jordan to possess and improve Information Security systems. It looks forward to achieve the following objectives:

1. Complete awareness of the Information Security management Systems impact on E-Business security, in force at financial institutions in Jordan.
2. Determining the impact of information security management systems (corporate security policies, frequent internal systems security audits, frequent external

systems security audits) which are subject to be violated by internal parties working in Jordanian banking Sectors.

3. Identifying the impact of information security management systems (corporate security policies, frequent internal systems security audits, frequent external systems security audits) which are subject to be violated by external parties in Jordanian banking Sector
4. Determining the impact of information security management systems (corporate security policies, frequent internal systems security audits, frequent external systems security audits) as to detecting intrusions in banking sector in Jordan.
5. Determining the impact of information security management systems (corporate security policies, frequent internal systems security audits, frequent external systems security audits) as to more secured system in banking sector in Jordan.

1.5 Study Model and Hypothesis.

The model (Figure 1-2) illustrates three independent variables (corporate security policies, frequently internal systems security audits, and external systems security audits). It also presents five dependent variables (E-business security firms, internal attacks vulnerability, external attacks vulnerability, intrusion detection success, having better security system). Moreover, it demonstrates the relationship between independent and dependent variables, and the extent of impact as to independent variables on dependent variables. The study hypotheses have been quoted from a previous study “An Exploratory Study on Systems Security and Hacker Hiring”, (Chan, & Yao, 2004):

- H01: There is no significant positive impact as to Information Security management Systems on E-Business security Banking Firms in Jordan at level ($\alpha \leq 0.05$).
- H02: There is no significant positive impact as to information security management's systems (corporate security policies, frequent internal systems security audits, frequent external systems security audits) on vulnerable to attacks*** by internal parties in banking Sector in Jordan at level ($\alpha \leq 0.05$).
- H03: There is no significant positive impact of information security management's systems (corporate security policies, frequent internal systems security audits, frequent external systems security audits) on vulnerable to **attacks by external parties in banking Sector in Jordan at level ($\alpha \leq 0.05$).

- H04: There is no significant positive impact of information security management's systems (corporate security policies, frequent internal systems security audits, frequent external systems security audits) **on successful at detecting intrusions in banking sector in Jordan at level ($\alpha \leq 0.05$).
- H05: There is no significant positive impact of information security management systems (corporate security policies, frequent internal systems security audits, frequent external systems security audits) **on better secure system in banking sector in Jordan at level ($\alpha \leq 0.05$).

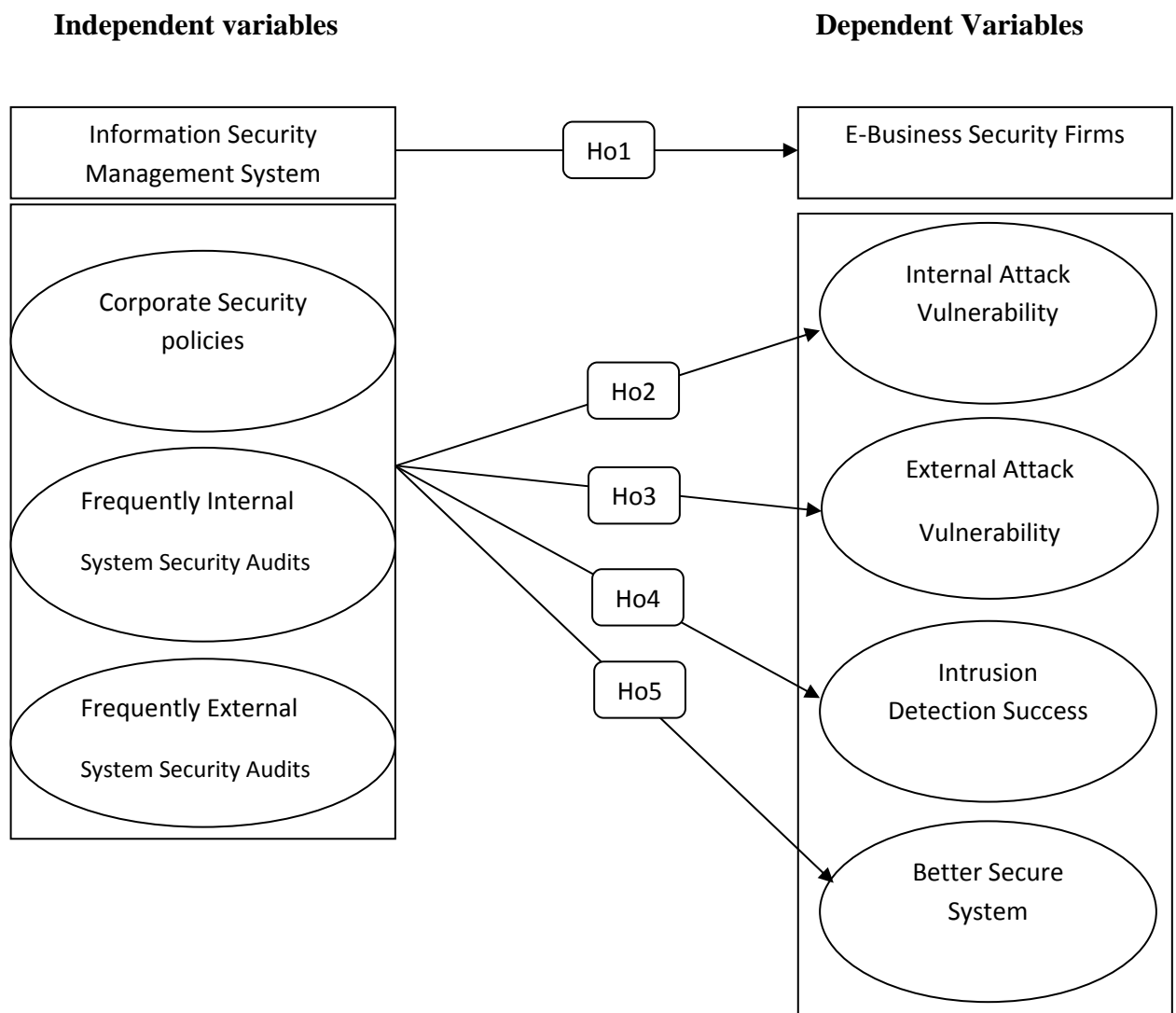


Figure 1-2 Study Model.

1.6: Study Limitations

Human Limitations: all the people and customer who are dealing with banking sector in Jordan.

Place Limitations: Banking sector in Jordan.

Scientific Limitations: The Research measures the impact of implementing Information Security Management System (ISMS), and uses Security Policies and Internal / External security audits controls on the suggested measures in e-business firms.

Time Limitations: The expected time to accomplish this study was limited to two academic semesters (2012-2013).

Access Limitation: accessing to new academic papers and Journals.

1.7: Study Delimitations (Difficulties).

1. The study concentrates on the Local Banks in Amman/Jordan; as a case study.
2. The accuracy of the study was based on collected information from the IT Department staff in Jordanian commercial banks.

1.8: Terminologies.

Information Security Management System (ISMS): Coordinated activities to direct and control the confidentiality, integrity, and availability of information. (Tipton & Krause, 2008)

- *Information*: Information is an asset that, like other important business assets, is essential to an organization's business, thus it further needs suitable protection. Information can be stored in many forms, including: digital form; electronic or optical medias, paperwork and employees diligences & expertise. Information may be transmitted by various means including, but not limited to; courier, electronic or verbal communication. Appropriate protection is required to be available in all information's transmission cases whatsoever. (ISO/IEC 27000, 2009).
- *Information Security*: Strict maintaining process which is in force in terms to the confidentiality, integrity, and availability of information. (Tipton & Krause, 2008).
- *E-Business*: any business which is run by digital processes through a computer network rather than physical space (Daft, 2010).
- *Corporate security policies*: Those policies which are available, to improve security process and “to address issues pertaining to system access controls, data confidentiality/privacy, and data integrity” (Locke & Hartley, 2001).
- *Frequently internal systems security audits*: provide firms with internal sense of security in that they may feel that their systems are more successful at detecting intrusions (Nevins, 2003).

- *Frequently External systems security audits*: audits aiming to detecting intrusions and violations practiced by T.P. (Cushing, 2001).
- *Internal attacks vulnerability*: These individuals may believe that firms with corporate security policies are less vulnerable to attacks by internal and external parties (Nevins, 2003).
- *External attacks vulnerability*: organizations with more frequent external systems security audit were perceived to be more successful at detecting intrusions, to have more secure systems or less vulnerable to attacks by external parties.

Chapter Two

Theoretical Framework and Previous Studies.

2.1 Introduction

2.2 Information

2.3 Information Security System.

2.4 Information Security Management System (ISMS)

2.5 E-Business

2.6 Literature review

2.7 Study Contribution to knowledge

2.1: Introduction.

Competition in certain industries has been transformed from company against company to supply-chain against supply-chain. Sharing information between organizations which are members on a supply-chain is a must. This information must be updated and accurate.

E-Business is a role which governs all organizations business and mode of its management. It touches processes, applications, staffs, infrastructure, business relations, sales, sales routing, domestic and foreign relations.. etc., however, the business cycles which used to be assessed on yearly basis is now assessed on daily basis. (Robertson & Sribar, 2004).

This chapter is intended to introduce:

- Information's definition, its importance as to the organization, elements, conceptual architecture, information's security incidents, and latest standardized information security processes and control works, transactions, and models. Also it introduces literature review.

2.2 Information:

Setting out the proper requirements and assessments to achieve the best security policies and obtain substantial protection to prevent any propane breaches and violations thereof.

Using Modern Technology in E-business requires a new security measures and policies to reduce the violations to the minimum degree, and maintaining the organization assets, through new technological and software applications via proper network devices.

The information security attacks of an organization's assets have high dollar impact, loss of customer confidence, and negative business goodwill. An organization must analyze its assets and the threats thereof, from either inside or outside violations.

Dealing through means that there is a need for new security policies to reduce the attacks and challenges imposed from these using e-business applications and devices, Information, network equipment, transmission media, computer systems, and servers are subject to threats. Use of e-business technologies has increased the incidents of computer attack. Security policies to protect organizations from different security attacks. To guarantee the security requirements of a given organization, it is essential to be able to evaluate the current security demands of an organization as well as the measures taken to achieve such requirements. Security weaknesses cause a negative impact on organizations such as financial loss, reputations, and loss of customer confidence (Kumar, Park, and Subramaniam, 2008).

Security management is required to safeguard information's confidentiality, integrity and accessibility. In order to achieve this issue, proper categorization of security

information level is requested to be focused on by those in charge of such process. (Chen, Shaw and Yang, 2006, Johnson, 2008 and. Nyanchama, 2005).

Collected data or information was plain text; i.e. readable. The only thing needed is to translate the data into English language. In 1971 they began to encrypt the data or information. Data interception still occurring, and new knowledge has been added to information war. The art of decoding encrypted data that has been intercepted.

They began encrypting that data using simple algorithms and methods. This did not prevent intercepted data to be interpreted, but it delays it until being decoded. Now day's encryption algorithms and methods became very complex. Decoding encrypted data takes hundreds of years using very powerful computers making the data expired and not important.

Information can be stored in different ways, including:

- Digital form, such as data files stored on electronic (Hard disks, and Tapes) or optical media (CDs, DVDs, Blu-ray).
- Material form; paperwork
- Unrepresented information in the form of knowledge of the employees.

Information can be transmitted and shared via different means, such as courier, electronic or verbal communication. Whatever form information takes, or the means by which information is transmitted, it always needs a proper protection.

Information and communication technologies are important for organization's information, and it is considered an essential element of the organization. These

technologies help and facilitate the creation, processing, storing, transmitting, protection and destruction of information.

Information threats and vulnerabilities increased these days causing billions of dollars damage. Computer-crimes and information-crimes are increasing with the extension and increasing of new communication technologies. Banking, government sector, and some global organization are victims of computer-crimes and information interception.

(Table 2-1) introduces a brief overview of major incidents from 1988 up to March 2004. (Egan & Mather 2005):

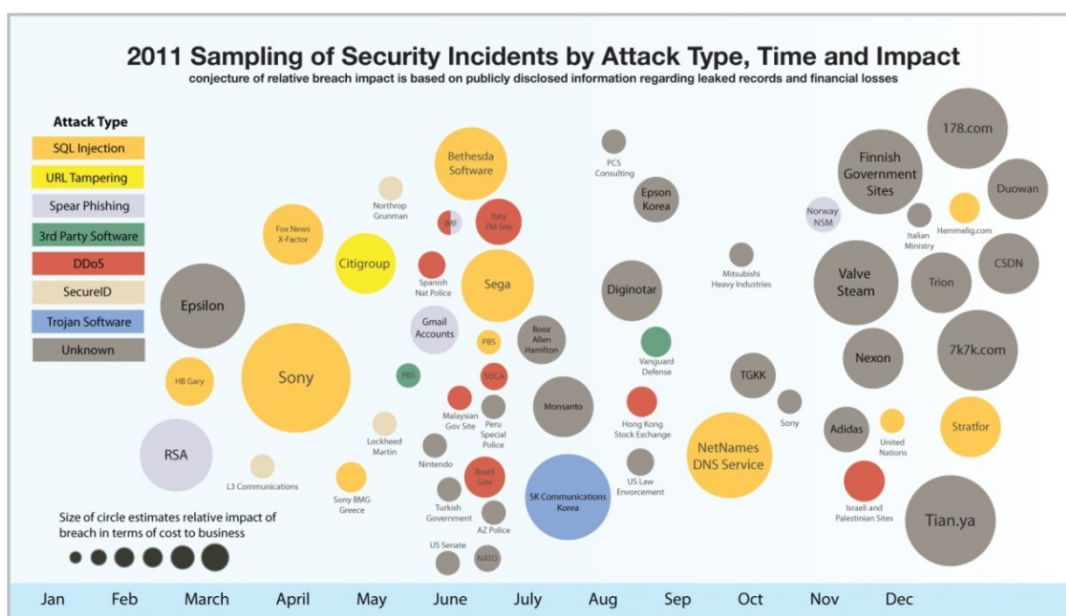
Table 2-1 Major Information Security Incidents. (Egan & Mather 2005)

Name	Date	Impact
Morris Worm	1988	<ul style="list-style-type: none"> • Stops 10% of computer connected to Internet
Melissa Virus	May 1999	<ul style="list-style-type: none"> • 100,000 computers in a week • \$1.5 billion impact
Explorer Virus	June 1999	<ul style="list-style-type: none"> • \$1.1 billion impact
Love Bug Virus (I love you virus)	May 2000	<ul style="list-style-type: none"> • \$8.75 billion impact
Sircam Virus	July 2001	<ul style="list-style-type: none"> • 2.3 million computers infected • \$1.25 billion impact
Code Red Worm	July 2001	<ul style="list-style-type: none"> • 359,000 computers infected in less than 14 hours • \$2.75 billion impact
Nimda Worm	Sept. 2001	<ul style="list-style-type: none"> • 160,000 computers infected at peak

Name	Date	Impact
		<ul style="list-style-type: none"> • \$1.5 billion impact
Klez	2002	<ul style="list-style-type: none"> • \$750 million impact
BugBear	2002	<ul style="list-style-type: none"> • \$500 million impact
Badtrands	2002	<ul style="list-style-type: none"> • \$400 million impact
Sapphire/Slammer Worm	Jan. 2003	<ul style="list-style-type: none"> • Infected 90% of vulnerable hosts in just 10 minutes • 75,000 hosts infected at peak • \$i.5 billion impact
Blaster	2003	<ul style="list-style-type: none"> • \$750 million impact
Nachi	2003	<ul style="list-style-type: none"> • \$500 million impact
soBig.F	2003	<ul style="list-style-type: none"> • \$2.5 billion impact
MyDoom Worm	Jan. 2004	<ul style="list-style-type: none"> • Fastest spreading mass-mailer worm to date. • 100,000 instance of the worm intercepted per hour • More than \$4.0 billion impact
Witty Worm	March 2004	<ul style="list-style-type: none"> • First widely propagated worm to carry a destructive payload

Internet user has grown to billions in the latest years. Organizations start appearing globally. The need of advance communication technologies are required to connect branches around the world to headquarters. This leads to increase the vulnerability of computer-crimes and information interference.

The below graph (Figure2-1) published by IBM X-Force shows 2011 sampling of security incidents by attack, time and impact. It also shows attack types, each attack has its own color. The size of circles estimates relative's impact of breach in terms of cost to business. SQL injection continued to be a major exploited weakness in targeted companies. December marked some of the largest impact-by-cost breaches that affected several massive social and entertainment sites in China with billions of dollars of potential losses.



Source: IBM X-Force® Research and Development

Figure 2-1 Sample of security incidents by attack type, time and impact. (IBM X-Force, 2012).

Recently a new RSA virus has been announced “Flame virus”. After planting it on victim computer, the virus becomes active by running a video or voice conference application such as Skype. The virus starts recording the session, and sends it to hacker. No antivirus application or hardware such as firewalls is able to detect and block it.

The need of securing organizations information becomes a priority. Also information security becomes a boardroom hot topic that is given high priority.

2.3 Information Security System.

The information management system and e-business technology systems and the networks, used for generating, storing and retrieving information and the human beings are important business assets of every organization. The security, integration and availability of information are essential for any banking organization to maintain its competitive edge, cash-flow, profitability, legal compliance and commercial image. The application of Information Technology has brought about significant changes in the way the banking and the financial organizations process and store data. The telecommunication networks have played a catalytic role in the expansion and integration of the Information Systems, within and among the organizations, facilitating data accessibility to different users. This has made it imperative for each organization to put in place adequate security controls to ensure data accessibility to all the authorized users, data inaccessibility to all the unauthorized users, maintenance of data integrity and implementation of all security threats to guarantee information and information systems security across the organization. This makes it necessary for each organization to define, document, communicate, implement and audit Information Systems Security (Information Technology, 2000).

In addition to other properties such as:

- *Authenticity*: “Property that an entity is what it claims to be”.
- *Accountability*: “Responsibility of an entity for its actions and decisions”.

- *Non-repudiation*: “Ability to prove the occurrence of claimed event or action and its originating entities, in order to resolve disputes about the occurrence or non-occurrence of event or action and involvement of entities in the event”.
- *Reliability*: “Property of consistent intended behavior and results”.

Transmission message from one individual co-worker, buyer, vendor, client, doctor, patient, relative at a remote location through several intermediate “nodes” before arriving at its final destination. At any point along the way, the contents of that e-mail could be visible to any number of people, including competitors, their agents, or individuals who would access the data for fraudulent purposes (Duane, 2004).

Information security has three major elements, people (staff and management), processes (business activities), and technology (IT, phones, pens ...). Figure 2-2 shows information security elements.

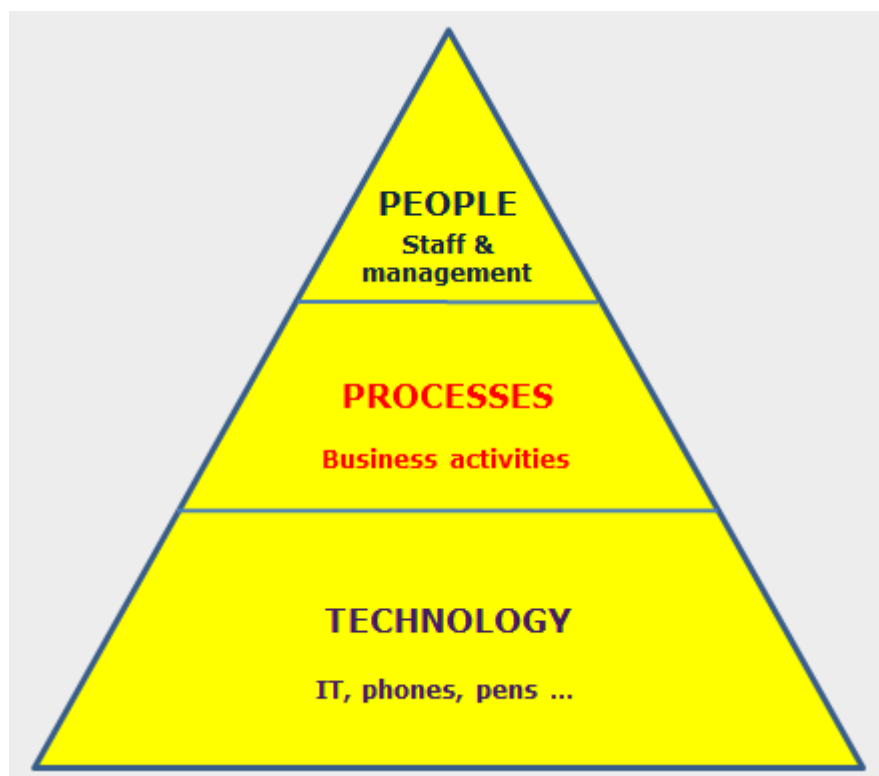


Figure 2-2 Information Security Elements. (Kamat, 2012).

- People: are those who use or have interest in your information security, people may be:
 - Shareholders (owners).
 - Management and staff.
 - Customers, clients, suppliers, and business partners.
 - Service providers, contractors, consultants, and advisors.
 - Authorities, regulators, and judges.

Threats may be originated from people (social engineers, unethical competitors, hackers, fraudsters, careless workers, bugs, flaws ...), on the other hand people are the organization biggest asset such as security-aware employees who spot trouble early.

- Processes: are work practices, workflows, steps, or activities needed to accomplish business objectives. (Kamat, 2012). Processes are described in procedures.

Securing information appropriately and repeatedly is defined by information security policies and procedures.

- Information technology includes:
 - Cabling, data/voice networks equipment.

- Telecommunications services (PABX, VoIP, ISDN, and videoconferencing).
- Phones, cellphones, PDAs.
- Computer servers, desktops, and associated data storage devices (disks, tapes).
- Paperwork, files.
- Pen and ink.

Information security technology includes:

- Locks, barriers, card-access systems, CCTV, and biometric systems.

Organizations can achieve Information Security by implementing an applicable set of controls. These controls are selected by through the chosen risk management process and managed using an Information Security Management Standard (ISMS), including processes, procedures, organizational structures, software and hardware to protect the identified information assets. Figure 2-3 introduce Information Security Conceptual Architecture and its components.

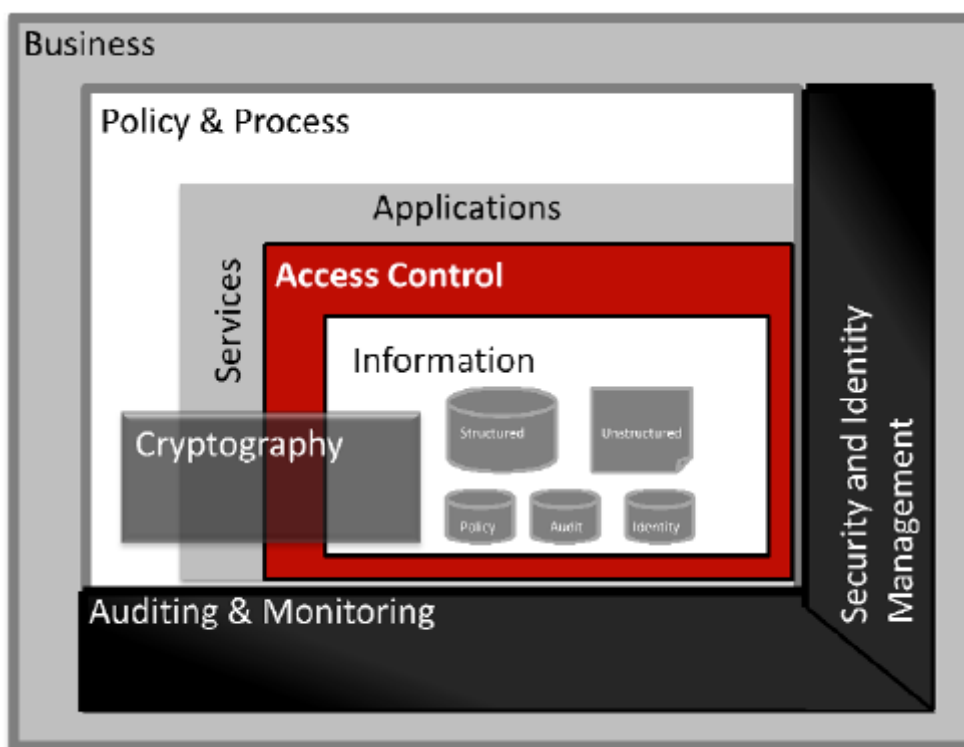


Figure 2-3 shows Information Security Conceptual Architecture. (Oracle, 2011)

As shown in Figure 2-3 Information is located at the center of the diagram, because as discussed before it is a valuable asset. The stored data as Information can be structured or unstructured. In addition the information scope also includes Policy and Process, Audit, and Identity information, which also needs to be secured.

Information is surrounded by Access Controls. Its task is to control, secure, and manage the access to Information.

Application or Service layer provides a way to interact with the information. It includes:

- Traditional business applications (e.g. Siebel), or SOA-based such as (secure) web service.
- Applications required managing Information Access Control, such as provisioning applications.

Policy and Process layer is responsible to specified and defined the rules that is used and deployed on Information Access Control, which controls the access to Information Layer by using applications and services.

Security & Identity Management, and Auditing & monitoring services are used to support the management and governance of the security within the Access Control layer, as well as the monitoring and remediation of those enforcement policies.

Cryptography is finally used to encrypt the data while it is moving across Information, Access Control, Services and Applications, and Polices & process layers.

2.4 Information Security Management System (ISMS).

Development of the Jordanian Banking Sector (2010)The Central Bank of Jordan carries out several tasks most important of which are issuing of banknotes security in the Kingdom, maintaining monetary stability, providing necessary liquidity for licensed banks and managing reserves of banks. It also seeks to enhance the security of the banking system institutions through various means of control. The Central Bank of Jordan focuses on achieving three national objectives which are: Contributing towards maintaining monetary and financial stability, promoting the sustained economic growth and social development of the kingdom in accordance with the general economic policy of the government, and contributing towards enhancing the investment environment. To

achieve the above-mentioned objectives, the Central Bank formulated six institutional goals that include: Maintaining a secure and well developed domestic payments system by maintaining the integrity and confidence in the Jordanian banks.

CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT (2001) the e-Banking architecture is hosted internally within the bank and is fully supported by various teams of technical support personnel. It consists of a tiered network infrastructure with various security controls in place to provide protection against insider and external attacks. The e-Banking application is written by an internal development team within the development environment. It is then migrated to the QA environment where it is tested (under-going both usability and stress testing) by a dedicated team of testers. It is also exposed to rigorous security testing by representatives from the Security Team. Once all necessary sign-off has been given the code is migrated to the production environment by the Webmasters.

The Webmasters also support and administer the web servers. The purpose of the policy is to ensure that all web servers, regardless of operating system, are built to a minimum, secure standard.

Vulnerability although the practice of segregation of duties is followed within Bank X job rotation and minimum leave are not enforced. Furthermore the logging capabilities in place are limited and could easily be manipulated by an administrator to cover up suspicious activity. The potential for collusion between technical team employees also exists

ISO/IEC 27000 (2009) defined *Information Security Management System (ISMS)* as: “Part of the overall management system, based on a business risk approach, to established, implement, operate, monitor, review, maintain and improve information

security”. Management System is “a framework of policies, procedures, guidelines, and associated resources to achieve the objectives of the organization”, and Information security is “preservation of confidentiality, integrity, and availability of information”.

Tipton & Krause, (2008) also defined *Information Security Management System (ISMS)* as: “Coordinated activities to direct and control the preservation of confidentiality, integrity, and availability of information”.

Information Security Management System (ISMS) family of standards consist of the following International Standards, under general title of “*Information Technology – Security Techniques*”: (ISO/IEC 27000, 2009)

- ISO/ IEC 27000:2009, *Information security management system – Overview and vocabulary.*
- ISO/ IEC 27001:2005, *Information security management system – Requirements.*
- ISO/IEC 27002:2005, *Code of practice for Information security management.*
- ISO/IEC 27003, *Information security management system implementation guidance.*
- ISO/IEC 27004, *Information security management — Measurement.*
- ISO/IEC 27005:2008, *Information security risk management.*
- ISO/IEC 27006:2007, *Requirements for bodies providing audit and certification of information security management system.*

- ISO/IEC 27007, *Guidelines for information security management systems auditing.*
- ISO/IEC 27011, *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002.*

NOTE: The general title “*Information technology - Security techniques*” indicates that these standards were prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

International Standards not under the same general title that are also part of the ISMS family of standards are as follows:

- ISO 27799:2008, *Health informatics — Information security management in health using ISO/IEC 27002*

Standards identified throughout these subclasses with no release year indicated are still under development.

The purpose and scope of ISMS family standard illustrated above can be found on “Appendix 1”.

ISO/IEC 27001, (2009) discuss the requirements to implement Information Security Management Systems. It uses Plan, Do, Check, and Act (PDCA) to achieve, maintain, and improve alignment of security with risks. Figure 2-4 describes Plan, Do, Check, and Act (PDCA) diagram.

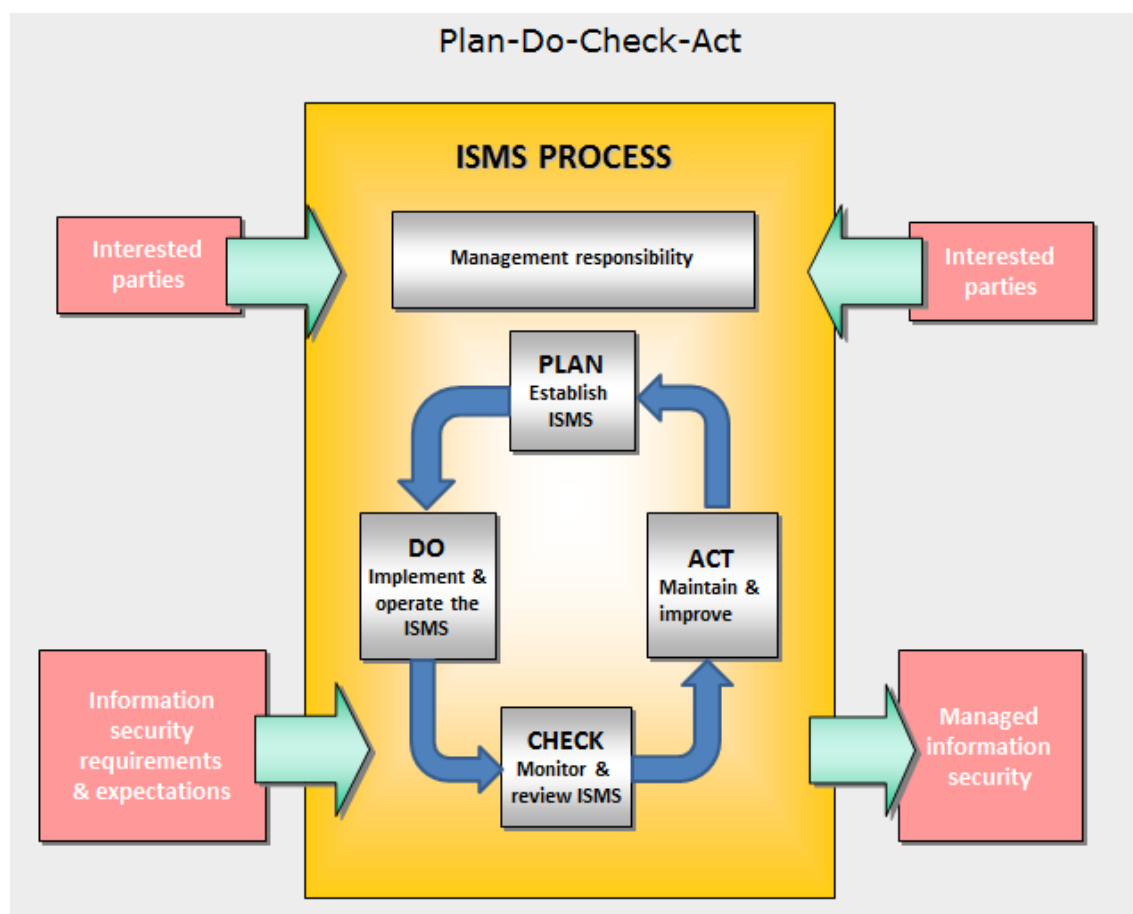


Figure 2-4 PDCA diagram (Kamat, 2012)

ISO/IEC 27000, (2009) defined *risk* as: “a combination of the probability of an event and its consequence”

Kamat, (2012) also defined *risk* as “the possibility that a threat exploits vulnerability in an information asset, leading to an adverse impact on the organization”, where threat is “something that might cause harm”, vulnerability is “a weakness that might be exploited”, and impact is a “financial damage etc.”

Figure 2-5 shows the relationship between Risk and vulnerabilities, threats, controls, Information assets, security requirements, and value.

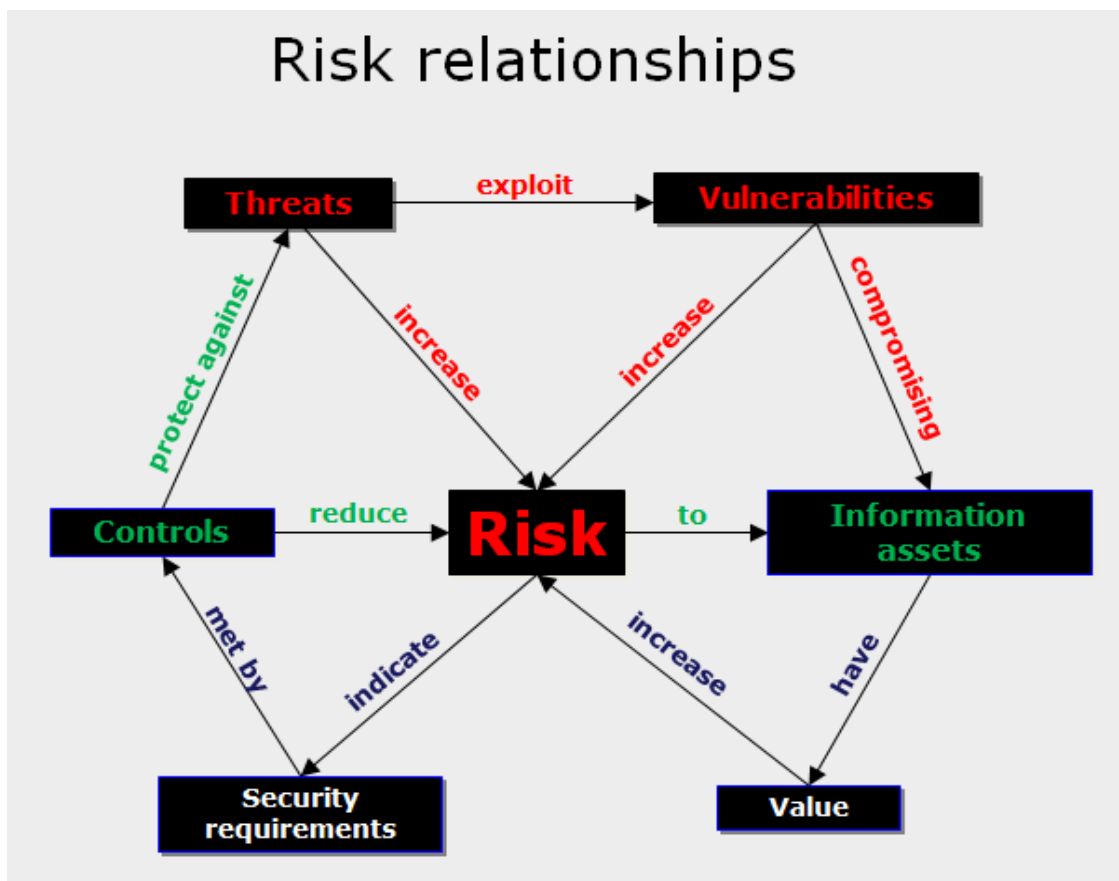


Figure 2-5 Risk relationships. (Kamat, 2012)

Once risk areas are identified, appropriate controls may be selected to mitigate these identified risk factors. ISO/IEC 27001:2005 identified the requirements to implement Information Security Management System (ISMS), also it illustrates the controls which are used as basis for the security risk assessment. Figure 2-6 illustrate controls clauses for Information Security Management Systems.



Figure 2-6 Control clauses. (Kamat, 2012)

Information Security Policy: address management support, commitment, and direction in accomplishing information security goals, including:

- Information Security Policy document.
- Ownership and review.

Organization of information security: addresses the need for a management framework that creates, sustains, and manages the security infrastructure, including:

- Management Information Security Forum.
- Information System Security Officer (ISSO).

- Information Security responsibilities.
- Authorization process.
- Organizational cooperation.
- Third-party access.
- Outsourcing.

Asset management: addresses the ability of the security infrastructure to protect organizational assets, including:

- Accountability and inventory.
- Asset classification based on business impact.
- Labeling.
- Handling, introduction, transfer, removal, and disposal of all assets.

HR security: addresses an organization's ability to mitigate risk inherent in human interactions, including:

- Personnel screening.
- Security responsibilities (code of conduct and non-disclosure agreements).
- Terms and conditions of employment.
- Training (information security awareness training program).
- Recourse a formal process to deal with violation of information security policies.

Physical and environmental security: addresses risk inherent to organizational premises, including:

- Location.
- Physical security perimeters.
- Access control.
- Equipment.
- Asset transfer.

Communication and operations management: addresses an organization's ability to ensure correct and secure operation of its assets, including:

- Operational procedures.
- Change control, process to manage change and configuration control, including change management of the Information Security Management System.
- Segregation and rotation of duties.
- Capacity planning, mechanism to monitor and project organizational capacity to ensure uninterrupted availability.
- System acceptance.
- Malicious code.
- Housekeeping.
- Network management.

- Media handling.
- Information exchange.

Access control: addresses an organization's ability to control access to assets based on business and security requirements, including:

- Business requirements: policy controlling access to organizational assets based on business requirements and "need to know".
- User management including:
 - Register and deregister users.
 - Control and review access and privileges.
 - Manage passwords.
- User responsibilities.
- Network access control including:
 - Authenticate nodes.
 - Authenticate external users.
 - Define routing.
 - Control network connections.
 - Maintain network segregation or segmentation.
 - Control network connections.
 - Maintain the security of network services.

- Host access control:
 - Automatically identify terminals.
 - Securely log-on.
 - Authenticate users.
 - Manage passwords.
 - Secure system utilities.
 - Furnish user duress capability, such as “panic buttons”.
 - Enable terminal, user, or connection timeouts.
- Application access control.
- Access monitoring.
- Mobile computing.

Information systems acquisition, development, and maintenance: addresses an organization’s ability to ensure that appropriate information system security controls are both incorporated and maintained, including:

- System security requirements.
- Application security requirements.
- Cryptography.
- System integrity.
- Development security.

Information security incident management: deal sensibly with security incidents that arise.

Business continuity management: addresses an organization's ability to counteract interruptions to normal operations, including:

- Business continuity planning.
- Business continuity testing.
- Business continuity maintenance.

Compliance: addresses an organizations ability to remain in compliance with regulatory, statutory, contractual, and security requirements, including:

- Legal requirements, awareness of:
 - Relevant legislation.
 - Intellectual property rights.
 - Safeguarding of organizational records.
 - Data privacy.
 - Prevention of misuse.
 - Regulation of cryptography.
 - Collection of evidence.
- Technical requirements.
- System audits.

Figure 2-7 illustrates Information Security Management System (ISMS) implementation process cycle.

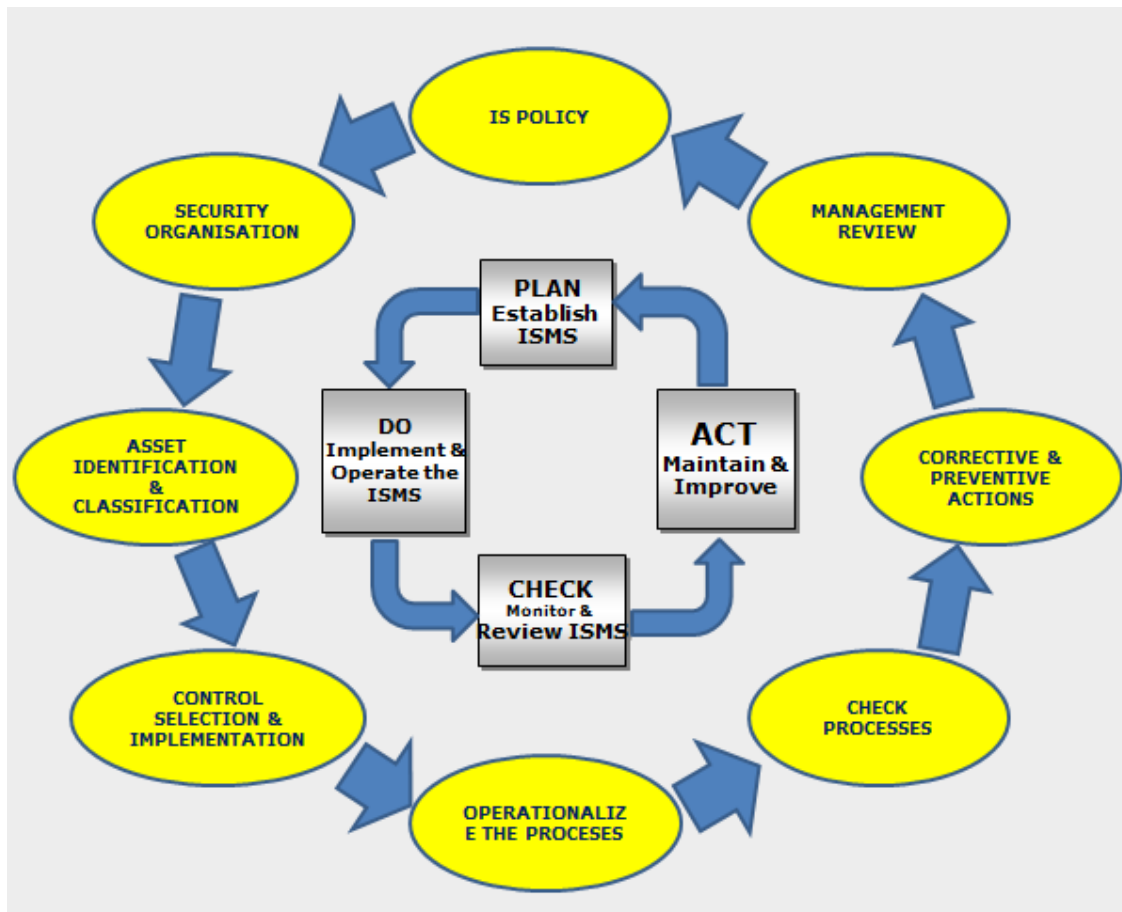


Figure 2-7 ISMS implementation process cycle. (Kamat, 2012)

2.5 E-Business.

E-business has technical components; management should be addressed regarding changes in organizational processes and interaction both within and outside a firm (Ash and Burn, 2003). For example, Raman et al. (2006) argued that organizational competitiveness is playing important roles in successful e-business implementation.

Examined that firm capabilities (such as information technology capability, strategic flexibility, and trust-building capability) are critical for superior firm performance in e-business firms. Moreover, developing organizational learning and knowledge management strategies has been considered an effective and efficient means of successful IT implementation (Lin and Lee, 2005). This perspective has been strengthened by several recent studies (Raymond and Blili, 2000; Malhotra et al., 2005; Ravichandran, 2005). However, empirical studies have seldom addressed the organizational capabilities (such as organizational learning and knowledge management capabilities) influencing e-business contribution to firm performance.

Simpson (2002) quoted in the OECD Global Forum that companies needed more importantly than ever to strengthen competitive capabilities based on productivity and innovation. This was based on three factors: intense international competition, the rapid pace of technological development, and the easy flow of investment and knowledge around the world.

Simpson (2002) quoted in the OECD Global Forum that companies needed more importantly than ever to strengthen competitive capabilities based on productivity and innovation. This was based on three factors: intense international competition, the rapid pace of technological development, and the easy flow of investment and knowledge around the world.

According to a study conducted by Forrester Research, an independent technology and market research company declares that: “online retail sales are projected to hit \$204 billion in 2008, up from \$175 billion in 2007, and should reach \$300 billion by 2013”. (Entrepreneur Magazine, 2012).

IBM was one of the first suppliers to use the term of E-business in 1997 to promote its services: “E-business is the transformation of key business processes through the use of Internet technology”.

Daft, (2010) defined E-business as “any business that takes place by digital processes over a computer network rather than in physical space”.

Entrepreneur magazine, (2011) declared that there are 10 reasons to place organization business online and to start running E-business:

- It is cheap. There is no less expensive way to open a business than to launch an online business.
- You cut your order fulfillment cost. There is no more efficient, cheap, fast, and accurate way to process orders via a website.
- Your catalog is always current. Updating printed catalog is too expensive, while an online catalog can be updated in minutes.
- High printing and mailing costs are history. Focus your marketing efforts on e-mail, newsletters, and online advertising rather than direct mail.
- You cut stuffing cost. A website can be a low-manpower operation. Once your website is online, its maintenance can be done by an independent contractor; which is much easier option than hiring a regular full-time employee.

- You can stay open 24 hours a day.
- You are in front of a global audience. E-business website is a borderless marketplace. Reviewing website logs you will see visitors streaming in from everywhere.
- There are no city permits and minimal red-tape hassles. Small web business can be run without permits and with little government involves.
- It is fast. E-business website is easy and fast to build and publish it.
- It is easy to get your message out. Between your website and smart use of e-mail and online advertising, you will have a complete control over when and how your message goes out.

E-business transactions can be done between different parties. Including: (Turban, etel, 2005)

- Business-to-business (B2B). Both the seller and buyer are organizations.
- Collaborative commerce (c-commerce). Business partners collaborate electronically. Collaboration of this type frequently occurs between and among business partners along the supply chain.
- Business-to-consumer (B2C). The sellers are organization, the buyers are individuals.
- Consumer-to-business (C2B). The consumer makes known a need for a particular product or service, and suppliers compete to provide the product or service.

- Consumer-to-consumer (C2C). An individual sells products (or services) to other individuals.
- Intrabusiness (intraorganizational) commerce. An organization uses E-business internally to improve its operations such as Business-to-Employee (B2E).
- Government-to-citizens (G2C) and to others. The government provides services to its citizens via E-business technologies.
- Mobile commerce (m-commerce). E-commerce done in a wireless environment, such as using cell phones to access the Internet.
- Social Commerce (SC). The delivery of E-business activities and transactions through social networks and/ or via Web 2.0 software.

Each of the above types of E-business is executed in one or more business models, including: (Turban Efraim, Aronson E. Jay, Liang Ting Peng, 2005).

- Online direct marketing: manufactures or retailers sell direct to customers.
- Electronic tendering systems: business conduct online tendering, requesting quotes from suppliers.
- Name-your-own-price: customers decide how much they are willing to pay. An intermediary (e.g. priceline.com) tries to match a provider.
- Find the best price: customers specify a need. An intermediary (e.g. hotwire) compares providers and shows the lowest price. Customer must accept in a specified time or lose the deal.

- Affiliate marketing: vendors ask partners to place logos (or banners) on partners' site. If customers click, come to vendors, and buy, vendors pay commission to partners.
- Viral marketing: spread your brand on the Net by word-of-mouth.
- Group purchasing (e-coops): aggregating the demands of small buyers to get a large volume.
- Online auctions: placing auctions on various types on the Internet.
- Product customization: using the Internet to self-configure products or services, price them, and then fulfill them quickly (build-to-order).
- Electronic marketplaces and exchanges: create virtual marketplace (private or public) where transactions can be conducted in an efficient way (more information to buyers and sellers, less transaction cost).
- Value-chain integrators: aggregates information and packages it for customers, vendors, or others in the supply chain.
- Value-chain service providers: specialized services in supply-chain operations, such as logistics or payment services.
- Information brokers: providing services related to E-business information, such as trust, content, matching buyers and sellers, evaluating vendors and products.
- Bartering online: exchanging surplus products and/or services that is completely administered online.

- Dip discounts: gain marketshare via dip discount (e.g. half.com) for customers that only consider price in their purchasing decisions.
- Membership model: only members can use the service provided, including access to certain information, and conducting trades (e.g. egreetings.com).
- Supply-chain improves: restricting supply-chains to hubs, or other configuration. Increases collaboration, reduces delays, and smooth flows.

2.6 literature review

Eckert (2000) under title *“Mobile Devices In E-business –New Opportunities and New Risks.”*.

The study investigates the new opportunities as well as the new risks coming along with mobile personal devices deployed in E-business or E-Commerce transactions. Based on its characteristic features the study researchers describe their vision of a mobile device serving as a trusted, controllable, personal security module to be used in open system environments. Then they analyze the new points of attack coming along with these mobile devices. Their analysis will point up that using nowadays mobile devices for distributed computing exposes the mobile user to lots of security threats he should be aware of.

The researcher discussed the opportunities of using mobile devices as personal and trusted security models. The study introduced the new risks coming along with the mobile device technology, and it also defined the main mobile devices related vulnerability. It also introduced an overview over security services provided by current operating systems for mobile devices.

Smith & Jamieson (2006) under title *“Determining Key Factors in E-Government Information System Security”*.

The authors investigate the key drivers and inhibitors for information system security and business continuity management in E-Government. The purpose of their study was to determine the key issues that exist with ISS and Business Continuity Planning (BCP) processes for the whole of government and then rank and rate them accordingly. Based

on data collected from a broad cross-section of government organizations, the key implementation issues include awareness, active management support, training, and appropriate funding.

McClain (2008), under title *“The Acceptance and Effectiveness of Federal and State Information Security Regulations in Multi-Branch Community Banks: A Phenomenological Analysis Conducted in Central California”*

The researcher evaluated the effectiveness of the current scheme of information security regulation in six federally regulated California community banks (participants resultant from a population of eighteen such banks to whom invitations were submitted), assessing the acceptance of such federal and state mandates by those banks and potential improvement of such regulation to the end of enhanced information system security. This was done through a three-phase project; qualitative, and two quantitative.

Philip (2008) under title *“Using Luftman’s Strategic Maturity Model in Assessing the Strategic Alignment of Information Technology and Internal Auditing Department”*.

The researcher tested six hypotheses to show the relationship between IT and IA departments. The findings helped to explain why some organizations struggle while others have strong alignment between IT and IA departments when audits are carried out; and why the benefits of IT governance can be difficult to achieve.

The result of the study generally showed a positive relationship between the IT and the IA departments.

Alqatawna, ET. AL, (2009) under title “*E-Business Security: Methodological Considerations*”.

The study aims to answer the question of how security be incorporated in the problem situation to provide a trustworthy E-business environment which considers the needs and the requirements of E-business security stakeholders. The study tried to answer the following questions to achieve its objectives:

- How is security perceived in the context of E-business organization in the study environment? And what are the implications of their perception?
- How customers’ culture, attitudes, awareness, and education affect E-business security?
- What is the current role of the government regarding E-business security? And how it can be an effective partner in the problem area?
- What factors technology provision affects E-business?

Baker, ET. AL, (2010) under title “*2010 Data Breach Investigations Report*”:

The investigation illustrates information and reports about global security breaches on 2010, also compares the results with year 2009 and 2008. The investigation methodology was based on data collection by two parties Verizon and United States Secret Service (USSS). The data was analyzed and illustrated using graphs.

Zaharia, et al, (2010) under title “*Online Crime and the Regulation of Business on the Internet*”

This article emphasize the importance of process transparency in EM transactions, the adoption of new forms of ecommerce and e-business in small and medium-sized enterprises (SMEs), and strengthening formal surveillance online.

The overall results provide strong evidence for the ongoing drive to reduce fraud, the evolution and subsequent shift of consumer trust in EM, and the compounding global effect of electronic commerce.

Zhao & Johnson (2010) under title “*Managing information Access in Data-Rich Enterprise with Escalation and Incentives*”

The article proposed an escalation scheme with audits to increase flexibility while maintaining security. It used game-theoretic model to show that an incentives-based policy with escalation and audit can control both over entitlement and under entitlement while maintaining flexibility.

Dunkerley (2011), under title “*Developing an Information Systems Security Success Model for Organizational Context*”

The author suggested a model that has been tested using CFA and SEM techniques. The findings suggest that the relationship between the technical level and effectiveness level of the IS security success program is partially mediated through the semantic level.

These findings present a solid first step towards a further understanding of IS security success within organizations and should provide a foundation for further research within the IS security domain.

Danilescu (2011) under title *“E-Business Data Access Authorizing Architecture By Applying Trusting Policies”*

Accessing data or information by internal or external parties is based on authentication and authorization. Authentication means asking for the user ID, and authorization involves checking the user privileges. The research refines an approach that defines hierarchies on access rights based on trust that brings a new model for security information conveyed by the organization.

Karahroudy (2011) under title *“Security Analysis and Framework of Cloud Computing with Parity-Based Partially Distributed File System”*.

The author aimed to introduce cloud computing as a new paradigm. He defines cloud computing, its properties, its services, its structure, cloud providers, and cloud usage types. He also introduces cloud computing advantages and disadvantages.

Cloud computing is in its early stages. Many organizations are trying to migrate from traditional computing environment to cloud computing. The purpose of migration is to get advantage of cloud computing by:

- Offering massive scalability.
- Immediate availability.
- Low cost services.

On the other hand cloud computing and its technology, it also carries with it inherent new risks and vulnerability. Risks and vulnerabilities security may cause big damages and lose to organizations,

The author proposed a model, “the Partially Distributed File System with Parity Chunks”. This model aimed to save the budget at the same time to support green technology, with optimum number of file servers, by addressing all three aspect of security (Confidentiality, Integrity, and Accessibility).

Lee, ET. AL, (2011) under title “*Managing Consumer Privacy Concerns in Personalization: a Strategic Analysis of Privacy Protection*”.

The authors aimed that E-Commerce and Information Technology enable firms to make personalized offers to individual consumers based on information about the consumers. They also assumed that the collection and use of private information have caused serious concerns about privacy invasion by consumers, creating a personalization-privacy tradeoff.

In their study they take a game-theoretic approach to explore the motivation of firms for privacy protection and its impact on competition and social welfare in the context of product and price personalization.

Martin, ET. AL, (2011) under title “*Security Excellence from a Total Quality Management Approach*”.

The authors focus on the synergy of business and security requirements to create a global methodology or approach. The integration revolves around the concept of total quality management to measure the security posture and is based on the premise that security requirements must be aligned and fused with the business’ objectives.

The authors used the American National Institute of Standards and Technology’s metrics are used as benchmarks to determine the security areas that should be addressed while the

European Framework for Quality Management is used to reflect the integration with the National Institute of Standards and Technology's metrics and to represent the domains in a business excellence approach. Then to depict the merger between security and business domains along a TQM approach and to be transferable to any standard or regulation by being able to incorporate acceptable security requirements into the underlying framework; they used the international Standard ISO/IEC 17799 (Information technology – security techniques – Code of practice for information security management).

Shahibi & Fakeh (2011) under title “*Security Factor and Trust in E-Commerce Transaction*”

The authors discussed the importance of trust in the success of an E-Commerce company. The authors describe their study and findings on the security factors that influence the trust of potential customers. They rank the security elements that induce the trust and examine their relationship with their demographic factors. Finally they introduce some recommendations to E-Commerce companies on security elements that they must incorporate in their system and service so that they can build the trust of their potential customers and retain them.

(Yong Jick and alt, 2011) under title "**Profit-maximizing firm investments in customer information security**".

This study investigates in the significance of information and knowledge associated with handling this kind of information. Providing protection may reduce the risk of the loss and misuse of information, but it imposes some costs on both the firm and its customers. Nevertheless, customer information security breaches still may occur. They have several distinguishing characteristics: it is hard to quantify monetary damages,

customer information security breaches may be caused by intentional attacks, and the frequency of such incidents typically is low.

The result, predictive models and explanatory statistical analysis using historical data have not been effective. Researcher found out a profit optimization model for customer information security investments. Our approach is based on value and operational risk modeling from financial economics. The main results of this work are that provide guidance on the trade-offs between risk and return in customer information security investments, characterize customer information management security investment levels when the firm is able to pass some of its costs on to consumers.

Study conducted by **(IBM) (March 2012)**. ***“IBM X-Force 2011 Trend and Risk Report”***

The report highlights on the second half of year 2011 threats on section one. Section two introduces security intelligence, how attackers attack social media and social networks. Section three discusses software development security practices. Section four introduces emerging trends in security. The report is supported by graph that shows information based on analyzed data. It also describes deeply each attack type and its impact on firms.

2.7 Study Contribution to knowledge.

The current study examined the effect The Impact of Implementing Information Security Management Systems on E-Business Firms. None of the previous studies had examined it. Besides that, all previous studies were implemented either in of Jordan context. This study deals with banking sector in Jordan. To clarify what distinguishes the current study from previous studies, some comparisons have been made, which are presented as follows: Previous studies have either concentrated on security policies or audits.

This study on the other hand has tried to bring attention to both policies and audits in a firm's security system, also concerning the environment, all studies have been mainly conducted in American, European and Asian countries. In contrast, the current study was carried in an Arab country, namely Jordan. In addition, on overview of the broad bodies of literature reveals that there is lack of extensive research on this subject, this study is an attempt to bridge this certain gap.

Chapter Three

Method and Procedures

3-1: Introduction.

3-2: Study Methodology.

3-3: Study Population.

3-4: Study Tools and Data Collection.

3-5: Statistics treatment.

3-6: Validity and Reliability.

Chapter Three

Method and Procedures

3-1: Introduction.

In this chapter the researcher will describe in detail the methodology used in this study, and the study population and its sample. Next, the researcher explains the study tools and the way of data collections. After that, he discusses the statistical treatment that is used in analysis of the collected data. In the final section the validation of the questionnaire and the reliability analysis that is applied will be clearly stated.

3-2: Study Methodology.

Descriptive research involves collecting data in order to test hypotheses or to answer questions concerned with the current status of the subject of the study. Typical descriptive studies are concerned with the assessment of attitudes, opinions, demographic information, conditions, and procedures. The research design chosen for the study is the survey research. A survey is an attempt to collect data from members of a population in order to determine the current status of that population with respect to one or more variables. The Survey research of knowledge at its best can provide very valuable data. It involves a careful design and execution of each of the components of the research process.

The researcher designed a survey instrument that could be administered to selected subjects. The purpose of the survey instrument was to collect data concerning respondent's attitudes towards firms with corporate security policies, frequently internal audits, and frequently external audits.

3-3: Study Population.

To increase credibility, it is important to choose the sample that will represent the population under investigation. The population of the study is Jordanian commercial banks, namely (15) banks. On the other hand, the researcher chooses a random sample consisting of (116) IT Department employees in the Jordanian banks.

After distributing (116) questionnaires of the study sample, a total of (116) answered questionnaires were retrieved, of which (0) were invalid, Therefore, (116) answered questionnaires were valid for study.

3-4: Study Tools and Data Collection.

The current study is of two folds, theoretical and practical. In the theoretical aspect, the researcher relied on the scientific studies that are related to the current study. Whereas in the practical aspect, the researcher relied on descriptive and analytical methods using the practical manner to collect, analyze data and test hypotheses.

The data collection, manners analysis and programs used in the current study are based on two sources:

1. Secondary sources: books, journals, these are used to write the theoretical framework of the study.
2. Primary source: a questionnaire that was designed to reflect the study objectives and questions.

In this study, both primary and secondary data were used. The data collected for the model were through questionnaire. After conducting a thorough review of the literature pertaining to Corporate Security Policies, Frequently Internal Audits, and Frequently External audits, the researcher formulated the questionnaire instrument for this study.

The questionnaire instrumental sections are as follows:

Section One: Demographic variables. The demographic information was collected with closed-ended questions, through (6) factors (Age; Gender; Education level; Professional Experience; and Professional Certifications).

Section Two: Corporate Security Policies. This section measured the Corporate Security Policies through (5) dimensions (vulnerability to attacks by internal parties (Employees), vulnerability to attacks by external parties (non-employees), intrusion detection success, have more secure systems, and view system security as an important issue) each dimension measure through (5) on a Likert-type scale as follows:

Strongly Agree	Agree	Neutral	Disagree	Strongly disagree
5	4	3	2	1

Section Three: Frequently Internal Systems Security Audits. This section measured through (3) dimensions (vulnerability to attacks by internal parties (Employees), intrusion detection success, and has more secure systems) each dimension measure through (5) on a Likert-type scale as follows:

Strongly Agree	Agree	Neutral	Disagree	Strongly disagree
5	4	3	2	1

Section Four: Frequently External Systems Security Audits. This section measured through (3) dimensions (vulnerability to attacks by external parties (non-employees), intrusion detection success, and has more secure systems) each dimension measure through (5) on a Likert-type scale as follows:

Strongly Agree	Agree	Neutral	Disagree	Strongly disagree
5	4	3	2	1

3-5: Statistics treatment.

The data collected from the responses of the study questionnaire were used through Statistical Package for Social Sciences (SPSS) & Amos for analysis and conclusions.

Finally, the researcher used the suitable statistical methods that consist of:

- Percentage and Frequency.
- Cronbach Alpha reliability (k) to measure strength of the correlation and coherence between questionnaire items.
- Arithmetic Mean to identify the level of response study sample individuals to the study variables.
- Standard Deviation to Measure the responses spacing degree about Arithmetic Mean.
- Chi-square test to measure the impact of study variables on testing direct effects.
- Correlation test among dependent variables.
- Relative importance, assigning due to:

$$\textit{Class Interval} = \frac{\textit{Maximum Class} - \textit{Minimum Class}}{\textit{Number of Level}}$$

$$\textit{Class Interval} = \frac{5 - 1}{3} = \frac{4}{3} = 1.33$$

The Low degree from 1- less than 2.33

The Medium degree from 2.33 – 3.66

The High degree from 3.67 and above.

3-6: Validity and Reliability.

3-6-1: Validation

To test the questionnaire for clarity and to provide a coherent research questionnaire, a macro review that covers all the research constructs was accurately performed by academic reviewers from Middle East University specialized in Business Administration, Marketing, IT, and information system. Some items were added, based on their valuable recommendations.

Some others were reformulated to become more accurate and that is expected therefore to enhance the research instrument.

The academic reviewers are (6) and the overall percentage of respond is (100%), (see appendix “2”).

3-6-2: Study Tool Reliability

The reliability analysis applied to the level of Cronbach Alpha (α) is the criteria of internal consistency which was at a minimum acceptable level (Alpha \geq 0.60) suggested by (Sekaran, 2003). The overall Cronbach Alpha (α) = (0.865). Whereas the High level of variables Cronbach alpha (α) is to Vulnerability to attacks by external parties (non-employees) within Frequently External Auditing = (0.968). The lowest level of Cronbach alpha (α) is to Have more secure systems within Frequently External Auditing = (0.659). These results are the acceptable levels as suggested by (Sekaran, 2003). The results were shown in Table (3-1).

Table 3-1, Reliability of Questionnaire Dimensions

Reliability of Questionnaire Dimensions		
No.	Dimensions	Alpha Value (α)
1	Corporate Security Policies.	
1-1	Vulnerability to attacks by internal parties (Employees).	0.838
1-2	Vulnerability to attacks by external parties (non-employees).	0.890
1-3	Intrusion detection success.	0.884
1-4	Have more secure systems.	0
1-5	View system security as an important issue.	0.659
2	Frequently Internal Systems Security Audits.	
2-1	Vulnerability to attacks by internal parties (Employees).	0.707
2-2	Intrusion detection success.	0.919
2-3	Have more secure systems.	0.739
3	Frequently External Systems Security Audits	
3-1	Vulnerability to attacks by external parties (non-employees).	0.968
3-2	Intrusion detection success.	0.884
3-3	Have more secure systems.	0.814
Total		0.865

Chapter Four.

Analysis Result and Hypotheses Test.

4-1: Introduction.

4-2: Study Questions Answers

4-4: Study Hypotheses Test.

Chapter Four.

Analysis Result and Hypotheses Test.

4-1: Introduction.

According to the research objectives and framework presented in previous chapters, this chapter will describe the research results including some description for research sample demographic variables. In addition, advance statistical analysis to test the research questions and research hypotheses. The data analysis included description for demographic variables of research sample respondents and frequency tables for each of the demographic variable. ANOVA analysis and multiple regressions are used to test the research hypotheses.

4-2. Study Questions answers:

A. Demographic Variables of the research sample

Five demographic variables are included in this research (Age, Gender, level of education, professional experience, and professional Certificate). The results in (Table 4-1) show the distribution of the research sample according to demographic variables.

Table 4-1

Distribution of research sample according to demographic variables.

Variable	Frequency	Percent%
Gender		
Male	92	79.3
Female	24	20.7
Age		
30 years and less	68	58.6
31-40 years	40	34.5
41-50 years	8	6.9
Professional experience		
Less than 5 years	48	41.4
6-10 years	28	24.1
11-15 years	32	27.6
16 years and more	8	6.9
Professional Certificate		
Operating system	60	51.7
Network	52	44.8
Hardware	52	44.8
Applications developments	8	6.9
communications	32	27.6
Database	12	10.3
Security	28	24.1
Internet web	24	20.7
Help desk	16	13.8

Results in (Table 4-1) indicated that there were (116) respondents, (79.3%) Male while the remaining (20.7%) was female. It also showed that the majority of

respondents (108 out of 116) have age less than 40 years old. According to the table more than half of respondents have 15 years or more as a professional experience. The last demographic variable is the professional certificate, it is clear that our research respondents have various professional certificates that allow them to judge the security attacks whether the source is internal or external. To concluded that the research respondents based on the aforementioned demographic variables are able to assess the security challenges and represent relevant prospect to collect data from.

B. Independent variables descriptive statistics

The security policies in this research divided into three dimensions: the existence of corporate security policy, internal audit, and external audit. Table 2:4 showed that the distribution of the sample according to the existence of corporate security policy.

Table 4-2

Sample Distributions According to Security Policy

corporate policy

	Frequenc y	Percent	Valid Percent	Cumulative Percent
Valid Yes	95	81.9	81.9	81.9
No	21	18.1	18.1	100.0
Total	116	100.0	100.0	

(Table 4-2) showed that out of 116 respondents 95(81.9%) believed that their company has developed and implemented active Corporate security policy. Thus, shows that the companies aware the risk of internal and external threats or attacks. The corporate security policy in this study is considered a categorical variable and the respondents have to answer yes or no according to their perceptions of the existed corporate security policy. The second dimension of security policies and procedures is the existence of internal audit. The descriptive statistics of this dimension and items belonging to are shown in (Table 4-3).

Table 4-3
Descriptive Statistic of Internal Audit in the Research Sample.

	Freque ncy	Percent	Valid Percent	Cumulative Percent
Once a month	48	41.4	46.2	46.2
once every three months	8	6.9	7.7	53.8
Valid once a year	16	13.8	15.4	69.2
Rarely	12	10.3	11.5	80.8
Others	20	17.2	19.2	100.0
Total	104	89.7	100.0	
Missing System	12	10.3		
Total	116	100.0		

It is clear from (Table 4-3) that nearly 48 (41.4) of research sample does internal audit once a month. And nearly half of the research sample does internal audit at least once

every three months. Thus, it shows that the research companies aware and try to prevent their systems from any intrusions before it harm their information systems. The third dimension of security policy is external audit. The descriptive statistics of this dimension and items belonging to are shown in (Table 4-4).

Table 4-4
Descriptive Statistic of External Audit in the Research Sample.

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid				
Once a month	28	24.1	26.9	26.9
once every three months	8	6.9	7.7	34.6
once every six months	4	3.4	3.8	38.5
once a year	32	27.6	30.8	69.2
Rarely	16	13.8	15.4	84.6
Others	16	13.8	15.4	100.0
Total	104	89.7	100.0	
Missing				
System	12	10.3		
Total	116	100.0		

It is obvious from (Table 4-4) that the research sample does external audit but nearly 70% do that once a year. It can be concluded that not all the research sample do external audit but nearly two third do which showed that how the research companies aware the

important of external audit in preventing internal and external attacks and facilitate intrusions detections.

C. Dependent variable: the dependent variable in this study consist of four sub-variables: Internal attack vulnerability, external attack vulnerability, intrusions detections success, and having better secure system. The descriptive statistics for internal attack vulnerability is shown in (Table 4-5).

Table 4-5
Internal Attack Vulnerability

Item	Mean	Standard Deviation
Q1	3.20	1.30
Q2	3.04	1.03
Q3	2.86	1.16
Q4	2.86	1.16
Q5	2.80	1.12
Q6	2.40	1.11
Q7	4.00	0.85
Q8	3.93	0.80
Q9	4.00	0.85
Q10	4.70	0.54
Q11	3.90	0.90
Q12	3.57	0.95

It is clear from (Table 4-5) that the research respondents perceived that their companies are vulnerable to be attacked by employees. Most of the internal attack vulnerability

items have means above 2.50 the middle point of Likert scale which indicates that all the research respondents expect and experience attacks from employees. Not only are the attacks come from internal sources but also from external parties.

Table 4-6

External Attack Vulnerability for the Research Companies.

Item	Mean	Standard deviation
Q13	4.03	0.87
Q14	3.28	0.99
Q15	3.82	0.97
Q16	4.07	0.71
Q17	4.03	0.63
Q18	3.93	0.77
Q19	3.57	0.73
Q20	3.85	0.64
Q21	4.07	0.65

The results in (Table 4-6) showed that the research companies are vulnerable to be attacked by non-employees or external individuals. As the means of all the variable items are above 3 which show that the research respondents answers ranged between agree and strongly agree that their companies encounter external vulnerability attack come from external sources or non-employees attacks. However, it is important to protect organizations systems and detect the intrusions as soon as possible.

Table 4-7
Intrusions detection success

Item	Mean	Standard deviation
Q22	3.92	0.89
Q23	4.03	0.87
Q24	3.93	0.88
Q25	4.07	0.71
Q26	3.89	0.77
Q27	4.10	0.67

It is obvious from (Table 4-7) that the research companies are successful in detection any intrusion whether its source is internal or external. The table shows all the items have mean over than 3.89 which indicated that the research companies are successful in detecting intrusions. But the question is really the system secure enough.

Table 4-8
Viewing the System is Secure

Item	Mean	Standard deviation
Q28	3.96	0.69

It is clear from (Table 4-8) that the research respondents perceive their systems are secure enough. This can be attributed to the availability of corporate security policy, internal audit, and external audit.

4-4: Study Hypotheses Test.

Based on the research problem and research model, five hypotheses were formulated to be tested in this study. The researcher used Statistical Package for Social Sciences (SPSS 16). In order to test the impact of independent variables on dependent variables simple and multiple regressions were used.

H01: There is no significant positive impact of Information Security management Systems (Corporate Security policy, internal audit, and external audit) on *E-Business security Firms* in banking sector in Jordan information security management system on E-Business security firms.

The Simple Regression was used to determine the impact of information security system (Corporate Security policy, internal audit, and external audit) on E-business security firms in banking sector, as shown in table no. (4-9), which shows that the F Value is so small ($F=0.04$; $\alpha=0.84$) and is not significant at $\alpha=0.05$. Therefore, we cannot reject the null hypothesis that assumes that there is no significant positive impact of information security management system on E-Business security firms in banking sector. This result is an expected but because of the increasing numbers of internal and external attacks our research respondents believed that their organization system is subject to attacks.

Table 4-9
Simple Regression between information security management system and E-Business security firms.

R2	F value	Sig
0.11	0.04	0.84

H02: There is no significant positive impact of Information Security management Systems (Corporate Security policy, internal audit, and external audit) on *vulnerability of internal attack* in banking sector in Jordan at level ($\alpha \leq 0.05$).

The Stepwise Multiple Regression was used to determine the importance of each independent variable separately in contributing to the mathematical model that represents the impact of information security system (Corporate Security policy, internal audit, and external audit) on vulnerability of internal attack, as shown in table no. (4-10), which shows that the F Test is not significant (0.377; $\alpha = 0.77$) at $\alpha \leq 0.05$ which indicates that information security management system have no significant impact on vulnerability to internal attack. Thus, we cannot reject the null hypothesis that assume there is no significant positive impact of information security management system (corporate security policy, internal audit, and external audit) on vulnerability of internal attacks.

Table 4-10
Stepwise Multiple Regression test to identify the effect of security management system on vulnerability of internal attack.

Order of entry of independent elements in the equation to predict	R² =0.011	(F) Value=0.377		Sig=0.77
	B	Beta	T	Sig
Corporate Security policy	0.28	0.10	1.05	0.29
Internal audit	0.016	0.03	0.23	0.82
External audit	0.010	0.018	0.13	0.89

H03: There is no significant positive impact of information security management systems (corporate security policies, frequent internal systems security audits, frequent external systems security audits) on vulnerable to attacks by external parties in banking Sector in Jordan at level ($\alpha \leq 0.05$).

The Stepwise Multiple Regression was used to determine the importance of each independent variable separately in contributing to the mathematical model that represents the impact of information security system (Corporate Security policy, internal audit, and external audit) on vulnerability of internal attack, as shown in table no. (4-11), as shown in table no. (4-11), which shows that the F Test is significant (5.16; $\alpha = 0.002$) at which less than $\alpha \leq 0.05$. This indicates that information security management system have a significant positive impact on vulnerability to external attack. Thus, we can reject the null hypothesis that assume there is no significant positive impact of information security management system (corporate security policy, internal audit, and external audit) on vulnerability of internal attacks and accept the alternative one.

Table 4-11
Stepwise Multiple Regression test to identify the effect of security management system on vulnerability of external attack.

Order of entry of independent elements in the equation to predict	R² =0.13	(F) Value=5.16		Sig=0.002
	B	Beta	T	Sig
Corporate Security policy	0.34	0.13	1.37	0.17
Internal audit	0.17	0.34	2.70	0.008
External audit	0.27	0.47	3.72	0.00

H04: There is no significant positive impact of information security management systems (corporate security policies, frequent internal systems security audits, frequent external systems security audits) on successful at detecting intrusions in banking sector in Jordan at level ($\alpha \leq 0.05$).

The Stepwise Multiple Regression was used to determine the importance of each independent variable separately in contributing to the mathematical model that represents the impact of information security system (Corporate Security policy, internal audit, and external audit) on vulnerability of internal attack, as shown in table no. (4-12), which shows that the F Test ($F=1.47$; $\alpha= 0.22$) is not significant at $\alpha= 0.05$. Thus, it can be concluded that there is no significant impact for information security management system (Corporate security policy, internal audit, and external audit) on intrusions detection success. In other words, based on the results in table 4-12, we accept the null hypothesis and reject the alternative one that assume no significant positive impact between information security management system and intrusion detection success.

Table 4-12
Stepwise Multiple Regression test to identify the effect of security management system on intrusion detection success.

Order of entry of independent variables in the equation to predict variance in dependent variable.	R² =0.042	(F) Value =1.47		Sig =0.22
	B	Beta	T	Sig
Corporate Security policy	0.18	0.08	0.80	0.43
Internal audit	0.11	0.25	1.90	0.06
External audit	0.06	0.12	0.87	0.39

H05: There is no significant positive impact of information security management systems (corporate security policies, frequent internal systems security audits, frequent external systems security audits) on better secure system in banking sector in Jordan at level ($\alpha \leq 0.05$).

The Stepwise Multiple Regression was used to determine the importance of each independent variable separately in contributing to the mathematical model that represents the impact of information security system (Corporate Security policy, internal audit, and external audit) on better secure system, as shown in table no. (4-13), which shows that the F Test ($F=4.27$; $\alpha= 0.007$) is significant at $\alpha= 0.05$. Thus, it can be concluded that there is significant impact for information security management system (Corporate security policy, internal audit, and external audit) on viewing better secure system. The results also showed that out of the three information security management system only the external audit ($T= 2.82$; $\alpha= 0.00$ which is less than 0.05) that affect the perceptions of research respondents to view their organizations system better secure.

Table 4-13
Stepwise Multiple Regression test to identify the effect of security management system on viewing better secure system.

Order of entry of independent variables in the equation to predict variance in dependent variable.	R²	(F) Value=4.27		Sig=0.007
	B	Beta	T	Sig
Corporate Security policy	0.085	0.072	0.77	0.40
Internal audit	0.011	0.051	0.40	0.70
External audit	0.091	0.361	2.82	0.00

To summaries, the research respondents are only believe and trust the capabilities of external audit in preventing internal and external attacks and easily detect intrusions. However, it seems to be the existence of corporate security policy does not play a critical role in preventing internal and external attacks. This result can be explained as the existence of the policy is not enough but it should be active and should be more than one method to prevent any internal or external intrusions. The hypotheses testing show that internal audit and the existence of corporate security policy have no significant impact on preventing internal and external system attack. This result appeared counterproductive because the logic is as much as we have methods and techniques to keep organization information system secure from any internal or external intrusions but as long as the intrusion trend around the globe rising up it is normal the research respondents believe that with the existence of corporate security policy, internal audit, and external audit still feel their system is not secure enough and subject to internal and external attacks.

Chapter Five

Results and Recommendations.

5-1: Results.

5-2: Recommendations.

Chapter Five

Results and Recommendations.

5-1: Results

This study is directed to assess the impact volume of information security management system in terms of E-Business system's firms. Thus the in-hand research text is designed to review the impact of corporate policy, internal audit, external audit fulfillment and its turn in restricting the internal & external violations and breaches. Upon applying such presentation on the ground, the hypotheses assessment showed the following:

- 1- The absence of impact as to information security management system on E-Business security banking firms. The foregoing is derived from the increasing number of violations on worldwide level, which raise a point of the impossibility to achieve the 100% fulfillment.
- 2- Statistics derived from Tables 4-10 indicate no significance for F Test (0.377; $\alpha = 0.77$) at ($\alpha \leq 0.05$), which second the aforesaid in Item No. 1 above. Accordingly, the major solution falls on the employees in charger thereof who interact with the system on daily basis which qualify them to create measures to minimize such violations.
- 3- Tables 4-11 indicate that F Test is significant (5.16; $\alpha = 0.002$) which is less than ($\alpha \leq 0.05$), thus the respective system do have significant positive impact on combating external violations. However, and by virtue of our research; Internal

and external audits, rather than corporate policy serve to reduce external violations, which do not apply to corporate policy.

- 4- The insignificance stipulated for in Item No. 2 above applies also to tables 4-12, Test F ($F=1.47$; $\alpha= 0.22$) as well. The foregoing is attributed to new types of intrusion which are developed recently and make violation attempts neither easy to be detected nor defeated.
- 5- The statistical results in tables (4-13) show that the F Test ($F=4.27$; $\alpha= 0.007$) is significant at $\alpha= 0.05$. Therefore, a significant impact of information security management system (Corporate security policy, internal audit, and external audit) on viewing better secure system. This result is expected as soon the organization installs more methods and techniques in terms of security system and makes them available to concerned employees for viewing. This is adopted and referred to in our research to bring the security system into more reliability and security.

5-2: Recommendations

Based on the hypotheses tests, recorded results and further deliberations, we put forth the following recommendations:

1. Concerned in charge should seek various security techniques and methods to maintain enough security as to E-business firms system. Employing high standards of security systems shall allow employees and customers to interact with the system at minimum limit of risk. Therefore, high level of security system may guarantee high level of productivity.
2. Specialized training shall be offered to all concerned employees to either minimize or whip out the internal violations. Besides, there should be internal circulations issued to address implications which the employees may suffer of, and the loss

volume which the organization may be subject to and attributed to violations committed either by the organization individuals or from outsiders, and the outcomes for such losses shall be reflected on the employees earnings.

3. Internal and external audits shall work together side by side to maintain sufficient security as to safety system. These audits are recommended to be performed regularly via set out programs, and make it subject to annual renewal for updating purposes.
4. Managers should focus on deploying more security methods and procedures to ensure that employees will view better secure system. Form psychological point of view especially the number of internal attacks will be reduced as soon as employees perceive that their organizations deploy various security systems.

References

1. Ali, Muhammad Mahboob, Mohsin, Chowdhury, Sifat-E and Yasmeen Farzana (2004). "E-Business in the Globalized world with special reference to Bangladesh: An analysis", *Business Review*, Vol.4, No.1&2.
2. Alqatawna, J., Siddiqi, J., Akhgar, B., and Btoush, M. H., (2009). "E-Business Security: Methodological Considerations", *World Academy of Science, Engineering and Technology*, 49, 624 – 631.
3. Ash, C.G. and Burn, J.M. (2003), "A strategic framework for the management of ERP enabled e-business change", *European Journal of Operational Research*, Vol. 146 No. 2, pp. 374-87.
4. Baker, W., Goudie, M., Hutton, A., Hylender, C. D., Niemantsverdriet, J., Novak, C., Ostetag, D., Porter, C., Rosen, M., Sartin, B., Tippet, P., and United States Secret Services, (2010), "2010 Data Breach Investigations Report", *Verizon corporation*.
5. Carlos, T., (September 2001), "Information Security Management: Understanding ISO 17799", *Lucent Technologies Worldwide Services*.
6. Clarke, R. (2001), "Introduction to information security", available at: www.anu.edu.au/people/Roger.Clarke/EC/IntroSecy.html
7. Chan, S. H., and Yao, L. J., (2004), "An Exploratory Study On Systems Security And Hacker Hiring", *The Review of Business Information Systems*, 8 (4), 17 – 28.
8. Chen, C. C., Shaw, R. S., and Yang, S.C. (2006). Mitigating information security risks By increasing user awareness: A case study of information security awareness system. *Information Technology, Learning & Performance Journal*, 24, 1-14.

9. CODE OF PRACTICE for INFORMATION SECURITY MANAGEMENT [AS/NZS ISO/IEC 17799:2001] – Standards Australia/New Zealand – 2001 – ISBN: 0733738761
10. Cushing, K. (2001). “Would you turn to the dark side?” *Computer Weekly*
11. Daft, R. L., (2010), “*New Era of Management*”. (9th ed), USA, South-Western, Cengage Learning.
12. Danilescu, L., (2011), “E-Business Data Access Authorizing Architecture By Applying Trusting Policies”, *Euro Economica*, 28 (2), 73 – 77.
13. Duane E. Sharp, (2004), “*Information Security in the Enterprise*”, *Euerbach publications*.
14. Dunkerley, D. K. (2011), “*Developing an information systems security success model for organizational context*”. (Unpublished doctoral dissertation), Nova Southeastern University, USA.
15. Eckert, C. (2000). “Mobile Devices In E-business New Opportunities and New Risks”, *TU München, Institut für Informatik Arcisstr. 21, D-80290 München*.
16. Egan, M., Mather, T., (2005), “*The Executive Guide to Information Security*”. *Symantec press*.
17. Entrepreneur Magazine (2012), “E-Business: Entrepreneur’s Step by Step Startup Guide”. Entrepreneur press, New York. (1-12-2012) (on-line), available:

<http://books.google.jo/books?id=NP-R-OmfbUoC&pg=PT16&dq=e+business+book&hl=en&sa=X&ei=IDrLUI-tC-aN0AXJoIGQDA&ved=0CGIQ6AEwCDgK#v=onepage&q=e%20business%20book&f=false>

18. IBM X-Force (2012). “*IBM X-Force 2011 Trend and Risk Report*”. U.S.A.
19. ISO/IEC 27000, (2009), “Information technology - Security techniques - Information security management systems - Overview and vocabulary”, *ISO / IEC*.
20. Information Technology (Certifying Authorities) Rules, 2000 dated the 17th October, 2000 – Government of India
21. International Data Corporation, 2007. Worldwide IT Security Software, Hardware, and Services 2007–2011 Forecast: The Big Picture. International Data Corporation (Doc #210018).
22. ITGI (2006), Information Security Governance, Guidance for Boards of Directors and Executive Management, 2nd ed., IT Governance Institute, Rolling Meadows, IL.
23. Kamat, M., (2012). “*Security Awareness Seminar an Introduction to ISO27K*”. ISO27K Forum, (10-11-2012.) (On-line), available:
http://www.iso27001security.com/ISO27k_ISMS_implementation_and_certification_process.pptx
24. Karahroudy, A. A., (2011). “*Security analysis and framework of cloud computing with parity-based partially distributed file system*”. (Unpublished master thesis) East Carolina University, USA.
25. Kumar, R. L., Park, S., and Subramaniam, C.(2008). Understanding the value of countermeasures portfolios in information systems security. *Journal on Management Information Systems*, 25, 241-279.
26. Johnson, M. E. (2008). Information risk of inadvertent disclosure: An Analysis of File Richardson, R. CSI Computer Crime& Security Survey. Computer Security Institute.

27. Lee, D. J., Ahn, J. H., and Bang, Y., (2011), "Managing Consumer Privacy Concerns in Personalization: a Strategic Analysis of Privacy Protection". *MIS Quarterly*; 35 (2), 423-A8.
28. Lin, H.F. and Lee, G.G. (2005), "Impact of organizational learning and knowledge management factors on e-business adoption", *Management Decision*, Vol. 43 No. 2, pp. 171-88.
29. Locke, A. D., & Hartley, B. V. (2001, May). "Security as a process". *DM Review*. <http://www.dmreview.com>
30. Martin, C., Bulkan, A., and Klempt, P., (2011), "Security Excellence from a Total Quality Management Approach". *Total Quality Management & Business Excellence*; 22 (3), p345-371.
31. McClain, C. I., (June 2008), "*The acceptance and effectiveness of federal and state information security regulations in multi-branch community banks: A phenomenological analysis conducted in central California*". (Unpublished doctoral dissertation), Capella University, USA.
32. Nyanchama, M. (2005). Enterprise vulnerability management and its role in information security management. *Information Systems Security*, 14, 29-56.
33. Oracle Corporation, (2002) "Managing E-Business Security Challenges", *Oracle Corporation*.
34. Oracle (2005). "Best Practices for Securing Oracle E-Business Suite", *Oracle Corporation*.
35. Oracle (2011). "*Information Security: a Conceptual Architecture Approach*", *Oracle Corporation*.

36. Parker, R. (2003), "How to profit by safeguarding privacy", *Journal of Accountancy*, Vol. 195 No. 5, pp. 47-52.
37. Philip A. H., (2008), "*Using luftman's strategic maturity model in assessing the strategic alignment of information technology and internal auditing Department*". (Unpublished doctoral dissertation), Colorado Technical University, USA.
38. Raman, P., Wittmann, C.M. and Rauseo, N.A. (2006), "The role of organizational capabilities in successful CRM implementation", *The Journal of Personal Selling and Sales Management*, Vol. 26 No. 1, pp. 39-54
39. Robertson, B., Sribar, V., (2004), "*Enriching the Value Chain: Infrastructure Strategies Beyond the Enterprise*". *Intel Press IT Best Practice Series*.
40. Shahibi, M. S., And Fakeh, K. W., (2011), "Security Factor and Trust in E-Commerce Transaction". *Australian Journal of Basic & Applied Sciences*; 5 (12), 2028-2033.
41. Simpson, R. (2002), "E-business, the engine of innovation",
42. Smith, S., Jamieson, R., (2006), "Determining Key Factors in E-Government Information System Security". *Information Systems Management*; 23 (2), 23-32.
43. Tipton, H. F., Krause, M., (2008), "*Information Security Management Handbook*", (6th ed) 2, Auerbach Publications.
44. Turban, E., Sharda, R., Delen, D., (2010), "*Decision Support Systems and Intelligent Systems*". (9th ed) Person Prentice Hall.

45. Zaharia, C. G., Zahari, C., Tudorescu, N., Zaharia, I., (2010), "Online Crime and the Regulation of Business on the Internet", *Economics, Management & Financial Markets*; 5 (4), 238-243.
46. Zhao, X., Johnson, E., (2010), "Managing information Access in Data-Rich Enterprise with Escalation and Incentives", *International Journal of Electronic Commerce*, 15 (1), 79-112.

Appendices

Appendix 1

Information Security Management System (ISMS) family standards, scope and purpose:
(ISO/IEC 27000:2009)

Standards describing an overview and terminology:

ISO/IEC 27000:

Information technology — Security techniques — Information security management systems — Overview and vocabulary.

Scope: This International Standard provides to organizations and individuals:

- an overview of the ISMS family of standards;
- an introduction to information security management systems (ISMS);
- a brief description of the Plan-Do-Check-Act (PDCA) process; and
- Terms and definitions used throughout the ISMS family of standards.

Purpose: ISO/IEC 27000 describes the fundamentals of information security management systems, which form the subject of the ISMS family of standards, and defines related terms.

Standards specifying requirements:

ISO/IEC 27001:

Information technology — Security techniques — Information security management systems — Requirements.

Scope: This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized information security management systems (ISMS) within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

This International Standard is universal for all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations).

Purpose: ISO/IEC 27001 provides normative requirements for the development and operation of ISMS, including a set of controls for the control and mitigation of the risks associated with the information assets which the organization seeks to protect by operating its ISMS. Organizations operating ISMS may have its conformity audited and certified. The control objectives and controls from Annex A (ISO/IEC 27001) shall be selected as part of this ISMS process as appropriate to cover the identified requirements. The control objectives and controls listed in Table A.1 (ISO/IEC 27001) are directly derived from and aligned with those listed in ISO/IEC 27002 Clauses 5 to 15.

ISO/IEC 27006:

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

Scope: This International Standard specifies requirements and provides guidance for bodies providing audit and ISMS certification in accordance with ISO/IEC 27001, in addition to the requirements contained within ISO/IEC 17021. It is primarily intended to support the accreditation of certification bodies providing ISMS certification according to ISO/IEC 27001.

Purpose: ISO/IEC 27006 supplements ISO/IEC 17021 in providing the requirements by which certification organizations are accredited, thus permitting these organizations to provide compliance certifications consistently against the requirements set forth in ISO/IEC 27001.

Standards describing general guidelines:

ISO/IEC 27002:

Information technology — Security techniques — Code of practice for information security management.

Scope: This International Standard provides a list of commonly accepted control objectives and best practice controls to be used as implementation guidance when selecting and implementing controls for achieving information security.

Purpose: ISO/IEC 27002 provides guidance on the implementation of information security controls. Specifically Clauses 5 to 15 provides specific implementation advice and guidance on best practice in support of the controls specified in Clauses A.5 to A.15 of ISO/IEC 27001.

ISO/IEC 27003:

Information technology — Security techniques — Information security management system implementation guidance.

Scope: This International Standard will provide practical implementation guidance and provide further information for establishing, implementing, operating, monitoring, reviewing, maintaining and improving ISMS in accordance with ISO/IEC 27001.

Purpose: ISO/IEC 27003 will provide a process oriented approach to the successful implementation of the ISMS in accordance with ISO/IEC 27001.

ISO/IEC 27004:

Information technology — Security techniques — Information security management — Measurement.

Scope: This International Standard will provide guidance and advice on the development and use of measurements in order to assess the effectiveness of ISMS, control objectives, and controls used to implement and manage information security, as specified in ISO/IEC 27001.

Purpose: ISO/IEC 27004 will provide a measurement framework allowing an assessment of ISMS effectiveness to be measured in accordance with ISO/IEC 27001.

ISO/IEC 27005:

Information technology — Security techniques — Information security risk management

Scope: This International Standard provides guidelines for information security risk management. The approach described within this International Standard supports the general concepts specified in ISO/IEC 27001.

Purpose: ISO/IEC 27005 provides guidance on implementing a process oriented risk management approach to assist in satisfactorily implementing and fulfilling the information security risk management requirements of ISO/IEC 27001.

ISO/IEC 27007:

Information technology — Security techniques — Guidelines for information security management systems auditing

Scope: This International Standard will provide guidance on conducting ISMS audits, as well as guidance on the competence of information security management system auditors, in addition to the guidance contained in ISO 19011, which is applicable to managements systems in general.

Purpose: ISO/IEC 27007 will provide guidance to organizations needing to conduct internal or external audits of ISMS or to manage an ISMS audit program against the requirements specified in ISO/IEC 27001.

Standard describing sector-specific guidelines

ISO/IEC 27011:

Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

Scope: This International Standard provides guidelines supporting the implementation of Information Security Management (ISM) in telecommunications organizations.

Purpose: ISO/IEC 27011 provides telecommunications organizations with an adaptation of the

ISO/IEC 27002 guidelines unique to their industry sector which are additional to the guidance provided towards fulfilling the requirements of ISO/IEC 27001, Annex A.

ISO/IEC 27799:

Health informatics — Information security management in health using ISO/IEC 27002

Scope: This International Standard provides guidelines supporting the implementation of Information Security Management (ISM) in health organizations.

Purpose: ISO/IEC 27799 provides health organizations with an adaptation of the ISO/IEC 27002 guidelines unique to their industry sector which are additional to the guidance provided towards fulfilling the requirements of ISO/IEC 27001, Annex A.

Appendix 2

Names of arbitrators.

No.	Name	Specialization	Univercity
1	Prof. Dr. Abdel NaserNour.	Managerial Accounting	MEU
2	Prof.Dr. Kamel AL-Mugrabi.	Business Administrator	MEU
3	Prof. Mohammad AL- Nuiami.	Financial Accounting	MEU
4	Dr. Laith AL-Rubaie	Marketing	MEU
5	Dr. KamelHawajreh.	Business Administrator	MEU
6	Dr. MuthafarAljarah	Computer Science	MEU

Appendix 3

Questionnaire

Mr. /Mrs..... Greeting

The research purpose is to explore the impact of “*Implementing Information Security Management System at E-Business Firms*”

The Questionnaire is designed to collect information about your organization. I would be grateful if you could answer ALL questions as completely and accurately as possible.

Thanks for answering all the items in the Questionnaire.

Suhail H. Alabed.

First Section: Demographic characteristics

1. Age:

30 years or less	<input type="checkbox"/>	31 to 40 years	<input type="checkbox"/>
41 to 50 years	<input type="checkbox"/>	More than 51 years	<input type="checkbox"/>

2. Gender:

Male	<input type="checkbox"/>	Female	<input type="checkbox"/>
------	--------------------------	--------	--------------------------

3. Education:

Bachelor's Degree	<input type="checkbox"/>	Master's Degree	<input type="checkbox"/>
PhD	<input type="checkbox"/>		

4. Professional Experience:

Less than 5 years	<input type="checkbox"/>	6 to 10 years	<input type="checkbox"/>
11 to 15 years	<input type="checkbox"/>	More than 16 years	<input type="checkbox"/>

5. Professional Certifications:

Operating System	<input type="checkbox"/>	Network	<input type="checkbox"/>
Hardware	<input type="checkbox"/>	Application development	<input type="checkbox"/>
Communication	<input type="checkbox"/>	Database	<input type="checkbox"/>
Security	<input type="checkbox"/>	Internet / Web	<input type="checkbox"/>
Helpdesk	<input type="checkbox"/>	Trainer	<input type="checkbox"/>
ERP	<input type="checkbox"/>	Wireless	<input type="checkbox"/>
other	<input type="checkbox"/>		

Second section: Corporate Security Policies

No.	Item	Answer alternatives				
		Strongly agree أنتفوق كلياً	Agree أنتفوق	Neutral محايد	Disagree لا أنتفوق	Strongly disagree لا أنتفوق كلياً
Vulnerability to attacks by internal parties (Employees).						
1	To what extent do you think that important information has been intentional deleted from an employee device?					
2	To what extent do you think employees or contractors can access unauthorized information?					
3	To what extent have your network, services been intentional stopped or damaged by an employee or contractor?					
Vulnerability to attacks by external parties (non-employees).						
1	To what extent do you experience attempts to attack by external parties (non-employee)?					
2	To what extent do experience denial of service attacks by non-employee?					
3	To what extent has your network or services been intentional stopped or damaged by external parties?					
Intrusion detection success						
1	To what extent do your security policies are successfully able to detect an intruder before attack.					
2	To what extent do your security policies are successfully able to detect an intruder after attack.					
Have more secure systems						
1	To what extent do your security policies make my systems more secure?					

No.	Item	Answer alternatives				
		Strongly agree أُتفق كلياً	Agree أُتفق	Neutral محايد	Disagree لا أُنفق	Strongly disagree لا أُنفق كلياً
	View system security as an important issue					
1	To what extent do you consider your security system as important issue?					
2	To what extent do you consider security system expenses are fair enough?					
3	To what extent is your security team well trained and have good knowledge on their field?					

Third: frequent internal audits:

How often does your firm conduct an internal security audits to your information system?			
Once a month	<input type="checkbox"/>	Once every three months	<input type="checkbox"/>
Once every six months	<input type="checkbox"/>	Once a year	<input type="checkbox"/>
Rarely	<input type="checkbox"/>	Others	<input type="checkbox"/>

No.	Item	Answer alternatives				
		Strongly agree اتفق كليا	Agree اتفق	Neutral محايد	Disagree لا اتفق	Strongly disagree لا اتفق كليا
Vulnerability to attacks by internal parties (Employees).						
1	To what extent do auditing security logs protect my system from internal attacks?					
2	To what extent does auditing my biometric devices make me unprotected by internal parties?					
3	To what extent does auditing my security system make me feel safer from internal attacks?					
Intrusion detection success						
1	To what extent do auditing security logs help me detect intruders after attack?					
2	To what extent do auditing security logs help me detect intruders after attack?					
3	To what extent do auditing access controls make me identify unauthorized access to information?					
Have more secure systems						
1	To what extent do auditing expired application licenses make my security system untrusted?					
2	To what extent does auditing help me detect unwanted applications?					
3	To what extent does auditing help me improve my security system?					

Fourth: frequent external audits:

How often does your firm conduct an external security audits to your information system?			
Once a month	<input type="checkbox"/>	Once every three months	<input type="checkbox"/>
Once every six months	<input type="checkbox"/>	Once a year	<input type="checkbox"/>
Rarely	<input type="checkbox"/>	Others	<input type="checkbox"/>

No.	Item	Answer alternatives				
		Strongly agree أوافق كلياً	Agree أوافق	Neutral محايد	Disagree لا أوافق	Strongly disagree لا أوافق كلياً
Vulnerability to attacks by external parties (non-employees).						
1	To what extent do auditing security logs protect my system from external attacks?					
2	To what extent does auditing my security system make me feel safer from external attacks?					
Intrusion detection success						
1	To what extent do auditing security logs help me detect intruders before attack?					
2	To what extent do auditing security logs help me detect intruders after attack?					
More secure systems						
1	To what extent do auditing expired firewall licenses make my security system untrusted?					
2	To what extent does auditing make my system more secure?					